

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2001-22844
(P2001-22844A)

(43)公開日 平成13年1月26日(2001.1.26)

(51) Int.Cl. ⁷	識別記号	F I	テラコード [*] (参考)
G 0 6 F 17/60		G 0 6 F 15/21	3 3 0 5 B 0 4 9
13/00	3 5 4	13/00	3 5 4 D 5 B 0 8 9
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 D 0 4 4
			6 4 0 Z 5 J 1 0 4
G 1 1 B 20/10		G 1 1 B 20/10	H 9 A 0 0 1
審査請求 未請求 請求項の数84 O L (全 88 頁) 最終頁に続く			

(21)出願番号 特願平11-193561

(22)出願日 平成11年7月7日(1999.7.7)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 野中 聡

東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 江崎 正

東京都品川区北品川6丁目7番35号 ソニ
一株式会社内

(74) 代理人 100094053

井理士 佐藤 隆久

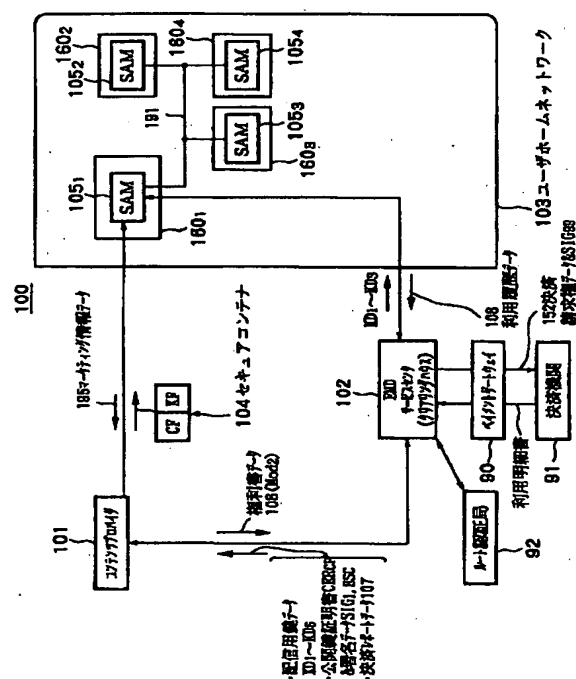
最終頁に続く

(54) 【発明の名称】 データ提供システムおよびその方法、管理装置およびデータ処理装置

(57) 【要約】

【課題】 データ提供装置の関係者の利益を保護できるデータ提供システムを提供する。

【解決手段】 コンテンツプロバイダ１０１は、コンテンツデータとその権利書データとを格納したセキュアコンテナ１０４をSAM１０５_１に配給し、SAM１０５_１は、配給を受けた権利書データに基づいて配給を受けたコンテンツデータの購入・利用形態を決定し、当該決定した購入・利用形態の履歴を示す利用履歴データ１０８をEMDサービスセンタ１０２に送信し、EMDサービスセンタ１０２は、利用履歴データ１０８に基づいて、ユーザが支払った金銭をコンテンツプロバイダ１０１の権利者に分配するための処理を行う。



1

【特許請求の範囲】

【請求項1】データ提供装置、データ処理装置および管理装置を有するデータ提供システムにおいて、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の係者に分配するための利益分配処理を行うデータ提供システム。

【請求項2】前記データ提供装置は、所定の鍵データを用いて前記コンテンツデータを暗号化して前記データ処理装置に配給し、

前記データ処理装置は、前記鍵データを用いて、前記受信したコンテンツデータを復号し、

前記管理装置は、前記鍵データを管理する請求項1に記載のデータ提供システム。

【請求項3】前記データ提供装置は、所定の鍵データを生成し、当該生成した鍵データを前記管理装置に登録し、

前記管理装置は、前記登録された前記鍵データを管理し、前記データ処理装置において、前記コンテンツデータの購入処理が行われたときに、対応する前記鍵データを前記データ処理装置に送信し、

前記データ処理装置は、受信した前記鍵データを用いて、前記受信したコンテンツデータを復号する請求項1に記載のデータ提供システム。

【請求項4】前記データ提供装置は、前記鍵データを暗号化し、当該暗号化した鍵データと前記暗号化したコンテンツデータと前記権利書データとを格納したモジュールを前記データ処理装置に配給する請求項2に記載のデータ提供システム。

【請求項5】前記管理装置は、配信用鍵データを管理し、前記配信用鍵データを前記データ提供装置および前記データ処理装置に配給し、

前記データ提供装置は、前記配信された前記配信用鍵データを用いて前記鍵データおよび前記権利書データを暗号化し、

前記データ処理装置は、前記配信された前記配信用鍵データを用いて前記鍵データおよび前記権利書データを復号する請求項4に記載のデータ提供システム。

【請求項6】前記管理装置は、各々所定の有効期限を持つ複数の前記配信用鍵データを、所定の期間分だけ、前

2

記データ提供装置および前記データ処理装置に配給する請求項5に記載のデータ提供システム。

【請求項7】前記データ提供装置は、前記暗号化したコンテンツデータおよび前記権利書データの少なくとも一方に対しての署名データを自らの秘密鍵データを用いて生成し、前記暗号化されたコンテンツデータ、前記暗号化した前記鍵データ、前記暗号化された前記権利書データおよび前記署名データを格納したモジュールを前記データ処理装置に配給し、

10 前記データ処理装置は、前記配給を受けた前記モジュール内に格納された前記署名データを、前記秘密鍵データに対応する公開鍵データを用いて検証し、

前記管理装置は、前記公開鍵データを管理する請求項4に記載のデータ提供システム。

【請求項8】前記データ提供装置は、前記自らの秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する請求項7に記載のデータ提供システム。

20 【請求項9】前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する請求項7に記載のデータ提供システム。

【請求項10】前記管理装置は、前記データ提供装置および前記データ処理装置に、それぞれ配信鍵データを配給し、

前記データ提供装置は、前記権利書データを、前記配信鍵データを用いて暗号化して前記データ処理装置に配給し、

30 前記データ処理装置は、前記配信鍵データを用いて、受信した前記権利書データを復号する請求項1に記載のデータ提供システム。

【請求項11】前記管理装置は、前記権利書データおよび前記鍵データの少なくとも一方の正当性を認証する請求項2に記載のデータ提供システム。

【請求項12】前記管理装置は、前記利益分配処理に応じた決済処理を行うことを請求する際に用いられる決済請求権データを生成し、当該決済請求権データに自らの秘密鍵データによる署名データを付加して、前記決済処理を行う装置あるいは前記データ提供装置に送信する請求項1に記載のデータ提供システム。

【請求項13】前記管理装置は、前記データ処理装置の登録処理を行い、登録された前記データ処理装置を管理し、前記登録された前記データ処理装置から受信した前記履歴データに基づいて前記利益分配処理を行う請求項1に記載のデータ提供システム。

50 【請求項14】前記データ処理装置は、前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態を決定し、当該決定した購入形態に応じた利用制御状態データを生成し、前記利用制御状態データに基づいて、前記配給を受けたコンテンツデータの利用を

3

制御する請求項1に記載のデータ提供システム。

【請求項15】前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールである請求項1に記載のデータ提供システム。

【請求項16】コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、

前記履歴データを前記データ処理装置から受信し、当該受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を行う管理装置。

【請求項17】所定の鍵データを用いて暗号化した前記コンテンツデータを、前記データ提供装置から前記データ処理装置に配給する場合に、

前記鍵データを管理する請求項15に記載の管理装置。

【請求項18】前記権利書データと、前記コンテンツデータを前記暗号化の際に用いる鍵データとの少なくとも一方の正当性を認証する請求項16に記載の管理装置。

【請求項19】コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、

前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記履歴データを前記管理装置に送信するデータ処理装置。

【請求項20】前記コンテンツデータが所定の鍵データを用いて暗号化されている場合に、前記鍵データを前記データ提供装置から受ける請求項19に記載のデータ処理装置。

【請求項21】処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールを用いて構成される請求項19に記載のデータ処理装置。

【請求項22】データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コン

4

テンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行うデータ提供システム。

【請求項23】前記データ提供装置は、前記コンテンツデータを、コンテンツ鍵データを用いて暗号化して前記データ配給装置に提供する請求項22に記載のデータ提供システム。

【請求項24】前記データ配給装置は、前記配給するコンテンツデータの価格を示す価格データを作成し、当該価格データを前記データ処理装置に配給する請求項22に記載のデータ提供システム。

【請求項25】前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを、配信鍵データを用いて暗号化して前記データ配給装置に提供し、

前記データ処理装置は、前記配信鍵データを用いて、前記コンテンツ鍵データおよび前記権利書データを復号し、

前記管理装置は、前記配信鍵データを管理し、前記配信鍵データを前記データ提供装置および前記データ処理装置に配給する請求項23に記載のデータ提供システム。

【請求項26】前記データ提供装置は、前記暗号化されたコンテンツデータ、前記暗号化されたコンテンツ鍵データおよび前記暗号化された前記権利書データの少なくとも一つのデータに対しての第1の署名データを自らの第1の秘密鍵データを用いて生成し、前記暗号化されたコンテンツデータ、前記暗号化された鍵データ、前記暗号化された権利書データおよび前記第1の署名データを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第1の秘密鍵データに対応する第1の公開鍵データを用いて前記第1の署名データを検証した後に、自らの第2の秘密鍵データを用いて生成した第2の署名データを前記第1のモジュールに格納

10

20

30

40

50

5

して第2のモジュールを生成し、当該第2のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記第1の公開鍵データを用いて、前記配給を受けた前記第2のモジュールに格納された前記第1の署名データを検証し、前記第2の秘密鍵データに対応する第2の公開鍵データを用いて、前記配給を受けた前記第2のモジュールに格納された前記第2の署名データを検証し、

前記管理装置は、前記第1の公開鍵データおよび前記第2の公開鍵データを管理する請求項25に記載のデータ提供システム。

【請求項27】前記データ提供装置は、前記第1の公開鍵データを格納した前記第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第1の公開鍵データおよび前記第2の公開鍵データを格納した前記第2のモジュールを前記データ処理装置に配給する請求項26に記載のデータ提供システム。

【請求項28】前記管理装置は、前記第1の公開鍵データおよび前記第2の公開鍵データを、前記データ処理装置に配給する請求項26に記載のデータ提供システム。

【請求項29】前記データ配給装置は、前記配給するコンテンツデータの価格を示す価格データを前記データ処理装置に配給し、

前記管理装置は、前記権利書データ、前記コンテンツデータを前記暗号化の際に用いる鍵データおよび前記価格データのうち少なくとも一つのデータの正当性を認証する請求項22に記載のデータ提供システム。

【請求項30】前記データ配給装置は、前記提供された暗号化されたコンテンツデータ、前記提供された権利書データ、前記コンテンツデータを暗号化した前記鍵データおよび前記配給されたコンテンツデータの価格を示す価格データとを格納したモジュールを、前記データ処理装置に配給する請求項22に記載のデータ提供システム。

【請求項31】前記管理装置は、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行って、決済を請求する際に用いられる決済請求権データを作成し、前記決済請求権データに自らの署名データを付加して、前記決済処理を行う装置に送信する請求項22に記載のデータ提供システム。

【請求項32】前記管理装置は、前記利益分配処理の結果を示す決済レポートデータを、前記データ提供装置および前記データ配給装置の少なくとも一方に送信する請求項31に記載のデータ提供システム。

【請求項33】前記管理装置は、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、およ

6

び、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行って、決済を請求する際に用いられる決済請求権データを作成し、前記決済請求権データに自らの署名データを付加して、前記データ提供装置および前記サービス提供装置の少なくとも一方に送信する請求項22に記載のデータ提供システム。

【請求項34】前記管理装置は、前記データ処理装置の登録処理を行い、登録された前記データ処理装置を管理し、前記登録された前記データ処理装置から受信した前記履歴データに基づいて前記利益分配処理を行う請求項22に記載のデータ提供システム。

【請求項35】前記データ処理装置は、前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態に応じた利用制御状態データを生成し、前記利用制御状態データに基づいて、前記配給を受けたコンテンツデータの利用を制御する請求項22に記載のデータ提供システム。

【請求項36】前記データ処理装置の前記第2のモジュールは、その処理内容、予め内部に記憶されたデータおよび処理中のデータを、外部から監視および改竄困難なモジュールである請求項22に記載のデータ提供システム。

【請求項37】コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う管理装置。

【請求項38】所定のコンテンツ鍵データを用いて暗号化した前記コンテンツデータを、前記データ提供装置から前記データ処理装置に配給する場合に、前記鍵データを管理する請求項37に記載の管理装置。

【請求項39】前記権利書データおよび前記コンテンツ鍵データの少なくとも一方の正当性を認証する請求項38に記載の管理装置。

【請求項40】コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの提供をデータ提供装置から受けたデータ配給装置から、前記コンテンツデ

7

ータおよび前記権利書データの配給を受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、
前記データ配給装置と通信を行う第1のモジュールと、
前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有するデータ処理装置。

【請求項41】 処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールからなる請求項40に記載のデータ処理装置。

【請求項42】 データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、
前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、
前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行い、
前記データ処理装置は、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第1のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信する第2のモジュールとを有し、
前記管理装置は、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配する利益分配処理を行うデータ提供システム。

【請求項43】 コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ配給装置を介してデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を前記管理装置用履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、

8

前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第1のモジュールと、

前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記管理装置用履歴データを前記管理装置に送信する第2のモジュールとを有するデータ処理装置。

【請求項44】 データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理するデータ提供システム。

【請求項45】 前記データ提供装置は、前記コンテンツデータの取り扱いを示す権利書データを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび権利書データを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記コンテンツデータを、前記配給を受けた前記権利書データに基づいて利用し、

前記管理装置は、ルート認証局に対して階層的に下に存在するサブ認証局の役割を果たし、登録された前記データ提供装置、前記データ配給装置および前記データ処理装置で用いられる秘密鍵データに対応する公開鍵データの正当性を証明する際に用いられる公開鍵証明書データの作成および管理と、前記権利書データの認証および前記コンテンツデータに関する権利処理とを行う請求項44に記載のデータ提供システム。

【請求項46】 前記データ提供装置は、前記鍵データを用いて暗号化して前記データ配給装置に提供し、
前記管理装置は、前記鍵データを管理する請求項45に記載のデータ提供システム。

【請求項47】 前記データ提供装置および前記データ配給装置の各々は、他の装置との間で認証を行う際に用いられる自らの秘密鍵データを作成し、当該作成した秘密鍵データを管理し、当該秘密鍵データに対応する公開鍵データを作成し、当該公開鍵データと身分証明書および決済口座を前記管理装置に登録し、

前記管理装置は、前記登録に応じて、前記公開鍵データの正当性を証明する公開鍵証明書データを作成する請求

項 4 5 に記載のデータ提供システム。

【請求項 4 8】前記管理装置は、前記登録に応じて、前記データ提供装置および前記データ配給装置に識別番号をそれぞれ割り振り、前記データ提供装置および前記データ配給装置に、ルート認証局の公開鍵データおよび管理装置の公開鍵データを送信する請求項 4 7 に記載のデータ提供システム。

【請求項 4 9】前記データ提供装置および前記データ配給装置の各々は、前記秘密鍵データをさらに前記管理装置に登録する請求項 4 7 に記載のデータ提供システム。

【請求項 5 0】前記データ処理装置には、前記管理装置が生成した秘密鍵データおよび当該秘密鍵データに対応する公開鍵データが予め格納されている請求項 4 5 に記載のデータ提供システム。

【請求項 5 1】前記データ処理装置には、前記管理装置が生成した前記公開鍵データの正当性を証明する公開鍵証明書データが予め格納されている請求項 5 0 に記載のデータ提供システム。

【請求項 5 2】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、
前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、
前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、
前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理するデータ提供システムにおいて、
前記データ提供装置、前記データ配給装置、前記データ処理装置および前記管理装置との間でのデータの伝送を、公開鍵暗号化方式を用いた相互認証、署名生成、署名検証と、共通鍵暗号化方式によるデータの暗号化とを用いて行うデータ提供システム。

【請求項 5 3】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、
前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、
前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、
前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他

の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理するデータ提供システムにおいて、

前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う前に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記他の装置に送信するデータ提供システム。

【請求項 5 4】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理するデータ提供システムにおいて、

前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う際に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記通信時に前記他の装置に送信するデータ提供システム。

【請求項 5 5】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを

用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、前記データ提供装置、前記データ配給装置および前記データ処理装置が前記公開鍵証明書破棄データが特定する公開鍵証明書データを用いた前記通信または前記配給を行うことを規制するデータ提供システム。

【請求項56】前記管理装置は、不正行為に用いられた前記データ提供装置、前記データ配給装置および前記データ処理装置に対応する公開鍵証明書データを特定する前記公開鍵証明書破棄データを生成する請求項55に記載のデータ提供システム。

【請求項57】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記配給を受けたコンテンツデータの利用を制御するデータ提供システム。

【請求項58】前記管理装置は、前記公開鍵証明書破棄データを前記データ処理装置に直接配給する請求項57に記載のデータ提供システム。

【請求項59】前記管理装置は、前記公開鍵証明書破棄データを、前記データ配給装置を介して、放送あるいはオンデマンド方式で前記データ処理装置に配給する請求項57に記載のデータ提供システム。

【請求項60】データ提供装置、データ配給装置、デー

タ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ配給装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記提供を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記提供されたコンテンツデータのの前記データ処理装置への配給を制御するデータ提供システム。

【請求項61】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、コンテンツデータの提供先のデータ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記データ配給装置への前記コンテンツデータの提供を制御する前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けたコンテンツデータを利用するデータ提供システム。

【請求項62】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置に

データを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータの提供し、

前記データ配給装置は、前記提供されたコンテンツデータと、前記配給を受けた公開鍵証明書破棄データとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御するデータ提供システム。

【請求項63】前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している請求項62に記載のデータ提供システム。

【請求項64】前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ配給装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前記配信用鍵データを用いて復号する請求項62に記載のデータ提供システム。

【請求項65】前記データ配給装置は、前記公開鍵証明書破棄データを、放送あるいはオンデマンド方式で前記データ処理装置に配給する請求項62に記載のデータ提供システム。

【請求項66】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処

理装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御するデータ提供システム。

【請求項67】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御するデータ提供システム。

【請求項68】データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データ

を生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御するデータ提供システム。

【請求項69】前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している請求項68に記載のデータ提供システム。

【請求項70】前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ提供装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前記配信用鍵データを用いて復号する請求項68に記載のデータ提供システム。

【請求項71】データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータと、前記配給された公開鍵証明書破棄データとを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御するデータ提供システム。

【請求項72】前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難

な構成を有している請求項71に記載のデータ提供システム。

【請求項73】前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ配給装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前記配信用鍵データを用いて復号する請求項71に記載のデータ提供システム。

10 【請求項74】データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記データ処理装置は、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データを前記管理装置に供給し、前記管理装置から供給された登録データ内の破棄フラグを参照して、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サー

20 ビスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合

に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを記憶し、当該公開鍵証明書破棄データに基づいて、前記データ処理装置から供給を受けた前記登録データ内の前記破棄フラグを設定して新たな登録データを生成し、当該生成した登録データを前記データ処理装置に配給し、

30 前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給するデータ提供システム。

【請求項75】データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

40 前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合

に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

50 前記データ提供装置は、前記データ配給装置にコンテン

ッデータおよび前記公開鍵証明書破棄データを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制するデータ提供システム。

【請求項 76】データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制するデータ提供システム。

【請求項 77】データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第 1 のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第 2 のモジュールとを

有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第 2 のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う決済機能と、前記権利書データの登録を行う権利管理機能とを有するデータ提供システム。

【請求項 78】前記管理装置は、前記決済機能を有する第 1 の管理装置と、前記権利管理機能を有する第 2 の管理装置とを有する請求項 77 に記載のデータ提供システム。

【請求項 79】前記決済は、電子決済である請求項 77 に記載のデータ提供システム。

【請求項 80】データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第 1 のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第 2 のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第 2 のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う際に用いられる決済請求権データを生成して前記データ配給装置に供給する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能とを有するデータ提供システム。

【請求項 81】データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

19

前記データ提供装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、

前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う際に用いられる決済請求権データを生成して前記データ提供装置に配給する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能とを有するデータ提供システム。

【請求項82】データ提供装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ処理装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、前記管理装置において、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行うデータ提供方法。

【請求項83】データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配

20

給し、

前記データ処理装置において、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置において、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行うデータ提供方法。

【請求項84】データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置において、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信し、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信し、

前記管理装置において、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配し、

前記データ配給装置において、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行うデータ提供方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンテンツデータを提供するデータ提供システムおよびその方法と、これらに用いられる管理装置およびデータ処理装置とに関する。

【0002】

【従来の技術】暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。このよ

21

うなデータ提供システムの一つに、音楽データを配信する従来のEMD(Electronic Music Distribution: 電子音楽配信)システムがある。

【0003】図67は、従来のEMDシステム700の構成図である。図67に示すEMDシステム700では、コンテンツプロバイダ701a, 701bが、サービスプロバイダ710に対し、コンテンツデータ704a, 704b, 704cと、著作権情報705a, 705b, 705cとを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報705a, 705b, 705cには、例えば、SCMS(Serial Copy Management System)情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ710の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

【0004】サービスプロバイダ710は、受信したコンテンツデータ704a, 704b, 704cと、著作権情報705a, 705b, 705cとをセッション鍵データを用いて復号する。そして、サービスプロバイダ710は、復号したあるいはオフラインで受け取ったコンテンツデータ704a, 704b, 704cに、著作権情報705a, 705b, 705cを埋め込んで、コンテンツデータ707a, 707b, 707cを生成する。このとき、サービスプロバイダ710は、例えば、著作権情報705a, 705b, 705cのうち電子透かし情報をコンテンツデータ704a, 704b, 704cに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにSCMS情報を埋め込む。さらに、サービスプロバイダ710は、コンテンツデータ707a, 707b, 707cを、鍵データベース706から読み出したコンテンツ鍵データKca, Kcb, Kccを用いてそれぞれ暗号化する。その後、サービスプロバイダ710は、暗号化されたコンテンツデータ707a, 707b, 707cを格納したセキュアコンテナ722を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置709に存在するCA(Conditional Access)モジュール711に送信する。

【0005】CAモジュール711は、セキュアコンテナ722をセッション鍵データを用いて復号する。また、CAモジュール711は、電子決済やCAなどの課金機能を用いて、サービスプロバイダ710の鍵データベース706からコンテンツ鍵データKca, Kcb, Kccを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置709において、コンテンツデータ707a, 707b, 707cを、それぞれコンテンツ鍵データKca, Kcb, Kccを用いて復号することが可能になる。このとき、CAモジュール711は、コンテンツ単位で課金処理を行い、その結果に

22

応じた課金情報721を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ710の権利処理モジュール720に送信する。この場合に、CAモジュール711は、サービスプロバイダ710が自らの提供するサービスに関して管理したい項目であるユーザの契約(更新)情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティ確保とを行う。

【0006】サービスプロバイダ710は、CAモジュール711から課金情報721を受信すると、サービスプロバイダ710とコンテンツプロバイダ701a, 701b, 701cとの間で利益配分を行う。このとき、サービスプロバイダ710から、コンテンツプロバイダ701a, 701b, 701cへの利益配分は、例えば、JASRAC(Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会)を介して行われる。また、JASRACによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【0007】また、端末装置709では、コンテンツ鍵データKca, Kcb, Kccを用いて復号したコンテンツデータ707a, 707b, 707cを、RAM型の記録媒体723などに記録する際に、著作権情報705a, 705b, 705cのSCMSビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ707a, 707b, 707cに埋め込まれたSCMSビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

【0008】

【発明が解決しようとする課題】ところで、SCMSは、CD(Compact Disc)からDAT(Digital Audio Tape)への録音を防止するために規定されたものであり、DATとDATとの間での複製が可能である。また、コンテンツデータに電子透かし情報を埋め込んだ場合も、問題が生じたときに、対象となっているコンテンツデータを提供したコンテンツプロバイダなどのコンテンツデータの流通経路を特定するに止まり、違法なコピーを技術的に阻止するものではない。従って、上述した図67に示すEMDシステム700では、コンテンツプロバイダの権利(利益)が十分に保護されないという問題がある。

【0009】また、上述したEMDシステム700では、ユーザの端末装置709からの課金情報721を、サービスプロバイダ710の権利処理モジュール720で処理するため、ユーザによるコンテンツデータの利用に応じてコンテンツプロバイダが受けるべき利益を、コンテンツプロバイダが適切に受けられるかどうか懸念される。

【0010】また、上述したEMDシステム700で

は、コンテンツプロバイダの著作権情報をサービスプロバイダがコンテンツデータに埋め込むため、コンテンツプロバイダは当該埋め込みが要求通りに行われているかを監査する必要がある。また、コンテンツプロバイダは、サービスプロバイダが契約通りに、コンテンツデータの配信を行っているかを監査する必要がある。そのため、監査のための負担が大きいという問題がある。

【0011】本発明は上述した従来技術の問題点に鑑みてなされ、コンテンツプロバイダの権利者（関係者）の利益を適切に保護できるデータ提供システムおよびその方法、管理装置およびデータ処理装置を提供することを目的とする。また、本発明は、コンテンツプロバイダの権利者の利益を保護するための監査の負担を軽減できるデータ提供システムおよびその方法、管理装置およびデータ処理装置を提供することを目的とする。

【0012】

【課題を解決するための手段】上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第1の観点のデータ提供システムは、データ提供装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う。

【0013】本発明の第1の観点のデータ提供システムでは、前記データ提供装置から前記データ処理装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを配給する。次に、データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する。次に、前記データ処理装置から管理装置に、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを送信する。次に、前記管理装置において、前記データ提供装置および前記データ処理装置を管理し、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う。

【0014】また、本発明の第2の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処

理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことによって得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

【0015】本発明の第2の観点のデータ提供システムでは、データ提供装置からデータ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供する。次に、前記データ配給装置からデータ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給する。次に、前記データ処理装置において、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する。次に、前記データ処理装置から前記管理装置に、前記決定した購入形態および利用形態の履歴を示す履歴データを送信する。次に、前記管理装置において、受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことによって得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

【0016】また、本発明の第3の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行い、前記データ処理装置は、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示

10

20

30

40

50

すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第1のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信する第2のモジュールとを有し、前記管理装置は、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配する利益分配処理を行う。

【0017】また、本発明の第4の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理する。

【0018】また、本発明の第5の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理するデータ提供システムであって、前記データ提供装置、前記データ配給装置、前記データ処理装置および前記管理装置との間でのデータの伝送を、公開鍵暗号化方式を用いた相互認証、署名生成、署名検証と、共通鍵暗号化方式によるデータの暗号化とを用いて行う。

【0019】また、本発明の第6の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用い

て作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理するデータ提供システムであって、前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う前に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記他の装置に送信する。

【0020】また、本発明の第7の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理するデータ提供システムであって、前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う際に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記通信時に前記他の装置に送信する。

【0021】また、本発明の第8の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装

置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、前記データ提供装置、前記データ配給装置および前記データ処理装置が前記公開鍵証明書破棄データが特定する公開鍵証明書データを用いた前記通信または前記配給を行うことを規制する。

【0022】また、本発明の第9の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記配給を受けたコンテンツデータの利用を制御する。

【0023】また、本発明の第10の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ配給装置は、前記管理装置から前記配給を受けた

公開鍵証明書破棄データに基づいて、前記提供を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記提供されたコンテンツデータの前記データ処理装置への配給を制御する。

【0024】また、本発明の第11の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、コンテンツデータの提供先のデータ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記データ配給装置への前記コンテンツデータの提供を制御し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けたコンテンツデータを利用する。

【0025】また、本発明の第12の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータの提供し、前記データ配給装置は、前記提供されたコンテンツデータと、前記配給を受けた公開鍵証明書破棄データとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給

29

した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する。

【0026】また、本発明の第13の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する。

【0027】また、本発明の第14の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果

30

に基づいて、前記配給を受けたコンテンツデータの利用を制御する。

【0028】また、本発明の第15の観点のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する。

【0029】また、本発明の第16の観点のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータと、前記配給された公開鍵証明書破棄データとを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する。

【0030】また、本発明の第17の観点のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記データ処理装置は、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データを前記管理装置に供給し、前記管理装置から供給された登録データ内の破棄フラグを参照して、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合には、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを記憶し、当該公開鍵証明書破棄データに基づいて、前記データ処理装置から供給を受けた前記登録データ内の前記破棄フラグを設定して新たな登録データを生成し、当該生成した登録データを前記データ処理装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給する。

【0031】また、本発明の第18の観点のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合には、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する。

【0032】また、本発明の第19の観点のデータ提供

システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合には、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する。

【0033】また、本発明の第20の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことによって得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う決済機能と、前記権利書データの登録を行う権利管理機能とを有する。

【0034】また、本発明の第21の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、

当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことによって得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う際に用いられる決済請求権データを生成して前記データ配給装置に供給する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能とを有する。

【0035】また、本発明の第22の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことによって得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う際に用いられる決済請求権データを生成して前記データ提供装置に配給する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能とを有する。

【0036】また、本発明の第1の観点の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、前記履歴データを前記データ処理装置から受信し、当該受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を行う。

【0037】また、本発明の第2の観点の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことによって得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

【0038】また、本発明の第1の観点のデータ処理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記履歴データを前記管理装置に送信する。

【0039】また、本発明の第2の観点のデータ処理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの提供をデータ提供装置から受けたデータ配給装置から、前記コンテンツデータおよび前記権利書データの配給を受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信する

35

データ処理装置であって、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有する。

【0040】また、本発明の第3の観点のデータ処理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ配給装置を介してデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を前記管理装置用履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第1のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記管理装置用履歴データを前記管理装置に送信する第2のモジュールとを有する。

【0041】また、本発明の第1の観点のデータ提供方法は、データ提供装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ処理装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを配給し、前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、前記管理装置において、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う。

【0042】また、本発明の第2の観点のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給し、前記データ処理装置において、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入

36

形態および利用形態の履歴を示す履歴データを前記管理装置に送信し、前記管理装置において、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの購入配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことによって得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

【0043】また、本発明の第3の観点のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置において、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信し、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信し、前記管理装置において、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配し、前記データ配給装置において、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行う。

【0044】

【発明の実施の形態】以下、本発明の実施形態に係わるEMD(Electronic Music Distribution: 電子音楽配信)システムについて説明する。

第1実施形態

図1は、本実施形態のEMDシステム100の構成図である。本実施形態において、ユーザに配信されるコンテンツ(Content)データとは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。図1に示すように、EMDシステム100は、コンテンツプロバイダ101、EMDサービスセンタ(クリアリング・ハウス、以下、ESCとも記す)102およびユーザホームネットワーク103を有する。ここで、コンテンツプロバイダ101、EMDサービスセンタ102、SAM1051~1054などが、それぞれ請求項1に係わるデータ提供装置、管理装置およびデータ処理装置に対応している。まず、EMDシステム100の概要について説明する。EMDシステム100で

は、コンテンツプロバイダ101は、自らが提供しようとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す権利書(UCP:Usage Control Policy)データ106を、高い信頼性のある権威機関であるEMDサービスセンタ102に送信する。権利書データ106は、EMDサービスセンタ102によって権威化(認証)される。

【0045】また、コンテンツプロバイダ101は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成すると共に、コンテンツ鍵データKcをEMDサービスセンタ102から配給された対応する期間の配信用鍵データKD1~KD56で暗号化する。そして、コンテンツプロバイダ101は、暗号化されたコンテンツ鍵データKcおよびコンテンツファイルCFと自らの署名データとを格納したセキュアコンテナ(モジュール)104を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などを用いて、ユーザホームネットワーク103に配給する。

【0046】ユーザホームネットワーク103は、例えば、ネットワーク機器1601およびAV機器1602~1604を有する。ネットワーク機器1601は、SAM(Secure Application Module)1051を内蔵している。AV機器1602~1604は、それぞれSAM1052~1054を内蔵している。SAM1051~1054相互間は、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルインタフェースバスなどのバス191を介して接続されている。

【0047】SAM1051~1054は、ネットワーク機器1601がコンテンツプロバイダ101からネットワークなどを介してオンラインで受信したセキュアコンテナ104、および/または、コンテンツプロバイダ101からAV機器1602~1604に記録媒体を介してオフラインで供給されたセキュアコンテナ104を対応する期間の配信用鍵データKD1~KD3を用いて復号した後に、署名データの検証を行う。SAM1051~1054に供給されたセキュアコンテナ104は、ネットワーク機器1601およびAV機器1602~1604において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。SAM1051~1054は、上述したセキュアコンテナ104の購入・利用の履歴を利用履歴(Usage Log)データ108として記録する。利用履歴データ108は、例えば、EMDサービスセンタ102からの要求に応じて、ユーザホームネットワーク103からEMDサービスセンタ102に送信される。

【0048】EMDサービスセンタ102は、利用履歴データ108に基づいて、課金内容を決定(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介

して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが決済機関91に支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101に支払われる。また、EMDサービスセンタ102は、一定期間毎に、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0049】本実施形態では、EMDサービスセンタ102は、認証機能、鍵データ管理機能および権利処理(利益分配)機能を有している。すなわち、EMDサービスセンタ102は、中立の立場にある最高の権威機関であるルート認証局92に対しての(ルート認証局92の下層に位置する)セカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ101およびSAM1051~1054において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ102の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、EMDサービスセンタ102は、コンテンツプロバイダ101の権利書データ106を登録して権威化することも、EMDサービスセンタ102の認証機能の一つである。また、EMDサービスセンタ102は、例えば、配信用鍵データKD1~KD6などの鍵データの管理を行なう鍵データ管理機能を有する。また、EMDサービスセンタ102は、権威化した権利書データ106に記述された標準小売価格SRP(Suggested Retailer's Price)とSAM1051~SAM1054から入力した利用履歴データ108とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ101に分配する権利処理(利益分配)機能を有する。

【0050】以下、コンテンツプロバイダ101の各構成要素について詳細に説明する。

【コンテンツプロバイダ101】図2は、コンテンツプロバイダ101の機能ブロック図であり、ユーザホームネットワーク103のSAM1051~1054との間で送受信されるデータに関連するデータの流れが示されている。また、図3には、コンテンツプロバイダ101とEMDサービスセンタ102との間で送受信されるデータに関連するデータの流れが示されている。なお、図3以降の図面では、署名データ処理部、および、セッション鍵データKsesを用いた暗号化・復号部に入出力するデータの流れは省略している。

【0051】図2および図3に示すように、コンテンツプロバイダ101は、コンテンツマスタソースサーバ111、電子透かし情報付加部112、圧縮部113、暗号化部114、乱数発生部115、暗号化部116、署名処理部117、セキュアコンテナ作成部118、セキュアコンテナデータベース118a、記憶部119、相

39

互認証部120、暗号化・復号部121、権利書データ作成部122、SAM管理部124およびEMDサービスセンタ管理部125を有する。コンテンツプロバイダ101は、EMDサービスセンタ102との間で通信を行う前に、例えば、自らが生成した公開鍵データ、自らの身分証明書および銀行口座番号（決済を行う口座番号）をオフラインでEMDサービスセンタ102に登録し、自らの識別子（識別番号）CP_IDを得る。また、コンテンツプロバイダ101は、EMDサービスセンタ102から、EMDサービスセンタ102の公開鍵データと、ルート認証局92の公開鍵データとを受け取る。以下、図2および図3に示すコンテンツプロバイダ101の各機能ブロックについて説明する。

【0052】コンテンツマスタソースサーバ111は、ユーザホームネットワーク103に提供するコンテンツのマスタソースであるコンテンツデータを記憶し、提供しようとするコンテンツデータS111を電子透かし情報付加部112に出力する。

【0053】電子透かし情報付加部112は、コンテンツデータS111に対して、ソース電子透かし情報(Source Watermark)Ws、コピー管理用電子透かし情報(Copy Control Watermark)Wcおよびユーザ電子透かし情報(User Watermark)Wuなどを埋め込んでコンテンツデータS112を生成し、コンテンツデータS112を圧縮部113に出力する。

【0054】ソース電子透かし情報Wsは、コンテンツデータの著作権者名、ISRCコード、オーサリング日付、オーサリング機器ID(Identification Data)、コンテンツの配給先などの著作権に関する情報である。コピー管理用電子透かし情報Wcは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。ユーザ電子透かし情報Wuには、例えば、セキュアコンテナ104の配給元および配給先を特定するためのコンテンツプロバイダ101の識別子CP_IDおよびユーザホームネットワーク103のSAM1051~1054の識別子SAM_ID1~SAM_ID4が含まれる。また、電子透かし情報付加部112は、必要であれば、検索エンジンでコンテンツデータの検索を行うためのリンク用のIDを電子透かし情報としてコンテンツデータS111に埋め込む。本実施形態では、好ましくは、各々の電子透かし情報の情報内容と埋め込み位置とを、電子透かし情報管理データとして定義し、EMDサービスセンタ102において電子透かし情報管理データを管理する。電子透かし情報管理データは、例えば、ユーザホームネットワーク103内のネットワーク機器1601およびAV機器1602~1604が、電子透かし情報の正当性を検証する際に用いられる。例えば、ユーザホームネットワーク103では、電子透かし情報管理データに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容

40

の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【0055】圧縮部113は、コンテンツデータS112を、例えば、ATrac3(Adaptive Transform Acoustic Coding 3)(商標)などの音声圧縮方式で圧縮し、圧縮したコンテンツデータS113を暗号化部114に出力する。

【0056】暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、DES(Data Encryption Standard)やTriple DESなどの共通鍵暗号化方式で、コンテンツデータS113を暗号化してコンテンツデータCを生成し、これをセキュアコンテナ作成部118に出力する。また、暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、A/V伸長用ソフトウェアSoftおよびメタデータMetaを暗号化した後に、セキュアコンテナ作成部117に出力する。

【0057】DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号化方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分(データ攪拌部)と、データ攪拌部で使用する鍵(拡大鍵)データを共通鍵データから生成する部分(鍵処理部)とからなる。DESの全てのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【0058】まず、平文の64ビットは、上位32ビットのH₀と下位32ビットのL₀とに分割される。鍵処理部から供給された48ビットの拡大鍵データK₁および下位32ビットのL₀を入力とし、下位32ビットのL₀を攪拌したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットのH₀と、F関数の出力との排他的論理和が算出され、その結果はL₁とされる。また、L₀は、H₁とされる。そして、上位32ビットのH₀および下位32ビットのL₀を基に、以上の処理を16回繰り返し、得られた上位32ビットのH₁₆および下位32ビットのL₁₆が暗号文として出力される。復号は、暗号化に使用した共通鍵データを用いて、上記の手順を逆さにたどることで実現される。

【0059】乱数発生部115は、所定ビット数の乱数を発生し、当該乱数をコンテンツ鍵データKcとして暗号化部114および暗号化部116に出力する。なお、コンテンツ鍵データKcは、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データKcは、例えば、所定時間毎に更新される。

【0060】暗号化部116は、後述するようにしてEMDサービスセンタ102から受信されて記憶部119に記憶された配信用鍵データKD₁~KD₆のうち対応

する期間の配信用鍵データKD₁～KD₆を入力し、当該配信用鍵データを共通鍵として用いたDESなどの共通暗号化方式によって図4(B)に示すコンテンツ鍵データK_c、権利書データ106、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃および署名・証明書モジュールMod₁を暗号化した後に、セキュアコンテナ作成部117に出力する。署名・証明書モジュールMod₁には、図4(B)に示すように、署名データSIG_{2,CP}～SIG_{4,CP}、コンテンツプロバイダ101の公開鍵データK_{CP,P}の公開鍵証明書CER_{CP}および当該公開鍵証明書CER_{CP}に対してのEMDサービスセンタ102の署名データSIG_{1,ESC}が格納されている。また、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃は、SAM105₁～105₄内でプログラムのダウンロードを行なう際に用いられるダウンロード・ドライバと、権利書データ(UCP)U106のシンタックス(文法)を示すUCP-L(Label)、R(Reader)と、SAM105₁～105₄に内蔵された記憶部(フラッシュROM)の書き換えおよび消去をブロック単位でロック状態/非ロック状態にするためのロック鍵データとを格納している。

【0061】なお、記憶部119は、例えば、公開鍵証明書データを記憶するデータベース、配信用鍵データKD₁～KD₆を記憶するデータベースおよびキーファイルKFを記憶するデータベースなどの種々のデータベースを備えている。

【0062】署名処理部117は、署名を行なう対象となるデータのハッシュ値をとり、コンテンツプロバイダ101の秘密鍵データK_{CP,S}を用いて、その署名データSIGを作成する。

【0063】なお、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値(出力)から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変換し、また、同一のハッシュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

【0064】セキュアコンテナ作成部118は、図4(A)に示すように、ヘッダデータと、暗号化部114から入力したそれぞれコンテンツ鍵データK_cで暗号化されたコンテンツデータC、A/V伸長用ソフトウェアSoftおよびメタデータMetaとを格納したコンテンツファイルCFを生成する。ここで、A/V伸長用ソフトウェアSoftは、ユーザホームネットワーク103のネットワーク機器160₁およびAV機器160₂～160₄において、コンテンツファイルCFを伸長する際に用いられるソフトウェアであり、例えば、ATRAC3方式の伸長用ソフトウェアである。

【0065】また、セキュアコンテナ作成部118は、図4(B)に示すように、暗号化部116から入力した対応する期間の配信用鍵データKD₁～KD₆で暗号化されたコンテンツ鍵データK_c、権利書データ(UCP)106およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC₃および署名・証明書モジュールMod₁を格納したキーファイルKFを生成する。そして、セキュアコンテナ作成部118は、図4(A)、(B)に示すコンテンツファイルCFおよびキーファイルKFと、図4(C)に示すコンテンツプロバイダ101の公開鍵データK_{CP}および署名データSIG_{1,ESC}とを格納したセキュアコンテナ104を生成し、これをセキュアコンテナデータベース118aに格納した後に、ユーザからの要求に応じてSAM管理部124に出力する。このように、本実施形態では、コンテンツプロバイダ101の公開鍵データK_{CP,P}の公開鍵証明書CER_{CP}をセキュアコンテナ104に格納してユーザホームネットワーク103に送信するイン・バンド(In-band)方式を採用している。従って、ユーザホームネットワーク103は、公開鍵証明書CER_{CP}を得るための通信をEMDサービスセンタ102との間で行う必要がない。なお、本発明では、公開鍵証明書CER_{CP}をセキュアコンテナ104に格納しないで、ユーザホームネットワーク103がEMDサービスセンタ102から公開鍵証明書CER_{CP}を得るアウト・オブ・バンド(Out-Of-band)方式を採用してもよい。

【0066】相互認証部120は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103との間でオンラインでデータを送受信する際に、それぞれEMDサービスセンタ102およびユーザホームネットワーク103との間で相互認証を行ってセッション鍵データ(共有鍵)K_{SES}を生成する。セッション鍵データK_{SES}は、相互認証を行う度に新たに生成される。

【0067】暗号化・復号部121は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103にオンラインで送信するデータを、セッション鍵データK_{SES}を用いて暗号化する。また、暗号化・復号部121は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103からオンラインで受信したデータを、セッション鍵データK_{SES}を用いて復号する。

【0068】権利書データ作成部122は、権利書データ106を作成し、これを暗号化部116に出力する。権利書データ106は、コンテンツデータCの運用ルールを定義した記述子(ディスクリプター)であり、例えば、コンテンツプロバイダ101の運用者が希望する標準小売価格SRP(Suggested Retailer' Price)やコンテンツデータCの複製ルールなどが記述されている。

【0069】SAM管理部124は、セキュアコンテナ

104を、オフラインおよび／またはオンラインでユーザホームネットワーク103に供給する。SAM管理部124は、CD-ROMやDVDなどのROM型の記録媒体(メディア)を用いてセキュアコンテナ104をオフラインでユーザホームネットワーク103に配給する場合には、配信用鍵データKD₁～KD₆などを用いてセキュアコンテナ104を暗号化して記録媒体に記録する。そして、この記録媒体は、販売などにより、ユーザホームネットワーク103にオフラインで供給される。

【0070】図5は、ROM型の記録媒体130を説明するための図である。図5に示すように、ROM型の記録媒体130は、ROM領域131、RAM領域132およびメディアSAM133を有する。ROM領域131には、図4(A)に示したコンテンツファイルCFが記憶されている。また、RAM領域132には、図4(B)、(C)に示したキーファイルKFおよび公開鍵証明書データCER_{CP}と機器の種類に応じて固有の値を持つ記録用鍵データKSTRとを引数としてMAC関数を用いて生成したと署名データと、当該キーファイルKFおよび公開鍵証明書データCER_{CP}とを記録媒体に固有の値を持つメディア鍵データK_{MED}を用いて暗号化したデータとが記憶される。また、RAM領域132には、例えば、不正行為などで無効となったコンテンツプロバイダ101およびSAM105₁～105₅を特定する公開鍵証明書破棄データ(リボケーションリスト)が記憶される。また、また、RAM領域132には、後述するようにユーザホームネットワーク103のSAM105₁～105₄においてコンテンツデータCの購入・利用形態が決定されたときに生成される利用制御状態(UCS)データ166などが記憶される。これにより、利用制御状態データ166がRAM領域132に記憶されることで、購入・利用形態が決定したROM型の記録媒体130となる。メディアSAM133には、例えば、ROM型の記録媒体130の識別子であるメディアIDと、メディア鍵データK_{MED}とが記憶されている。メディアSAM133は、例えば、相互認証機能を有している。

【0071】また、SAM管理部124は、セキュアコンテナ104を、ネットワークやデジタル放送などを用いてオンラインでユーザホームネットワーク103に配信する場合には、暗号化・復号部121においてセッション鍵データK_{SES}を用いてセキュアコンテナ104を暗号化した後に、ネットワークを介してユーザホームネットワーク103に配信する。本実施形態では、SAM管理部、EMDサービスセンタ管理部、並びに後述するコンテンツプロバイダ管理部およびサービスプロバイダ管理部として、例えば、内部の処理内容の監視(モニタリング)および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【0072】ここで、コンテンツプロバイダ101から

ユーザホームネットワーク103へのコンテンツデータCの配給は、上述したように記録媒体130を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ106が格納された共通の形式のセキュアコンテナ104を用いる。従って、ユーザホームネットワーク103のSAM105₁～105₄では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ106に基づいた権利処理を行なうことができる。

【0073】また、上述したように、本実施形態では、セキュアコンテナ104内に、コンテンツ鍵データK_Cで暗号化されたコンテンツデータCと、当該暗号化を解くためのコンテンツ鍵データK_Cとを同封するイン・バンド(In-Band)方式を採用している。イン・バンド方式では、ユーザホームネットワーク103の機器で、コンテンツデータCを再生しようとするときに、コンテンツ鍵データK_Cを別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データK_Cは配信用鍵データKD₁～KD₆で暗号化されているが、配信用鍵データKD₁～KD₆は、EMDサービスセンタ102で管理されており、ユーザホームネットワーク103のSAM105₁～105₅に事前に(SAM105₁～105₄がEMDサービスセンタ102に初回にアクセスする際に)配信されているので、ユーザホームネットワーク103では、EMDサービスセンタ102との間をオンラインで接続することなく、オフラインで、コンテンツデータCの利用が可能になる。なお、本発明は、コンテンツデータCとコンテンツ鍵データK_Cとを別々に、ユーザホームネットワーク103に供給するアウト・オブ・バンド(Out-Of-Band)方式を採用できる柔軟性を有している。

【0074】EMDサービスセンタ管理部125は、EMDサービスセンタ102から6カ月分の配信用鍵データKD₁～KD₆およびそれぞれに対応した署名データSIG_{KD1,ESC}～SIG_{KD6,ESC}と、コンテンツプロバイダ101の公開鍵データK_{CP,P}を含む公開鍵証明書CER_{CP}およびその署名データSIG_{1,ESC}と、決済レポートデータ107とを受信すると、これらを暗号化・復号部121においてセッション鍵データK_{SES}を用いて復号した後に、記憶部119に記憶する。決済レポートデータ107は、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の内容が記述されている。

【0075】また、EMDサービスセンタ管理部125は、提供するコンテンツデータCのグローバルユニーク(Global Unique)な識別子Content__ID、公開鍵データK_{CP,P}およびそれらの署名データSIG_{9,CP}を、EMDサービスセンタ102に送信し、EMDサービスセンタ102から、公開鍵データK_{CP,P}の公開

45

鍵証明書データCER_{CP}を入力する。また、EMDサービスセンタ管理部125は、権利書データ106をEMDサービスセンタ102に登録する際に、図6(A)に示すように、提供するコンテンツデータCのグローバルユニークな識別子Content_ID、コンテンツ鍵データK_cおよび権利書データ106を格納したモジュールMod₃と、その署名データSIG_{5,CP}とを格納した権利書登録要求用モジュールMod₂を作成し、これを暗号化・復号部121においてセッション鍵データK_{SES}を用いて暗号化した後に、ネットワークを介してEMDサービスセンタ102に送信する。EMDサービスセンタ管理部125としては、前述したように、例えば、内部の処理内容の監視(モニタリング)および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【0076】以下、図2および図3を参照しながら、コンテンツプロバイダ101における処理の流れを説明する。なお、以下に示す処理を行う前提として、コンテンツプロバイダ101の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ102に登録処理を行い、グローバルユニークな識別子CP_IDを得ている。識別子CP_IDは、記憶部119に記憶される。

【0077】まず、コンテンツプロバイダ101が、EMDサービスセンタ102に、自らの秘密鍵データK_{CP,S}に対応する公開鍵データK_{CP,P}の正当性を証明する公開鍵証明書データCER_{CP}を要求する場合の処理を図3を参照しながら説明する。まず、コンテンツプロバイダ101は、真性乱数発生器を用いて乱数を発生して秘密鍵データK_{CP,S}を生成し、当該秘密鍵データK_{CP,S}に対応する公開鍵データK_{CP,P}を作成して記憶部119に記憶する。EMDサービスセンタ管理部125は、コンテンツプロバイダ101の識別子CP_IDおよび公開鍵データK_{CP,P}を記憶部119から読み出す。そして、EMDサービスセンタ管理部125は、識別子CP_IDおよび公開鍵データK_{CP,P}を、EMDサービスセンタ102に送信する。そして、EMDサービスセンタ管理部125は、当該登録に応じて、公開鍵証明書データCER_{CP}およびその署名データSIG_{1,ESC}をEMDサービスセンタ102から入力して記憶部119に書き込む。

【0078】次に、コンテンツプロバイダ101が、EMDサービスセンタ102から配信用鍵データを受信する処理を図3を参照しながら説明する。なお、以下に示す処理を行う前提として、コンテンツプロバイダ101は、EMDサービスセンタ102から既に公開鍵証明書データCER_{CP}を得ている必要がある。EMDサービスセンタ管理部125が、EMDサービスセンタ102から6カ月分の配信用鍵データKD₁~KD₃およびその署名データSIG_{KD1,ESC}~SIG_{KD6,ESC}を入力し、

46

これを記憶部119内の所定のデータベースに記憶する。そして、署名処理部117において、記憶部119に記憶された署名データSIG_{KD1,ESC}~SIG_{KD6,ESC}の正当性が確認された後に、記憶部119に記憶されている配信用鍵データKD₁~KD₆が有効なものとして扱われる。

【0079】次に、コンテンツプロバイダ101がユーザホームネットワーク103のSAM105₁にセキュアコンテナ104を送信する場合の処理を図2を参照しながら説明する。なお、以下の例では、コンテンツプロバイダ101からSAM105₁にセキュアコンテナ104を送信する場合を例示するが、セキュアコンテナ104をSAM105₂~105₄に送信する場合も、SAM105₁を介してSAM105₂~105₄に送信される点を除いて同じである。まず、コンテンツデータS111がコンテンツマスタソースサーバ111から読み出されて電子透かし情報付加部112に出力される。次に、電子透かし情報付加部112は、コンテンツデータS111に電子透かし情報を埋め込んでコンテンツデータS112を生成し、これを圧縮部113に出力する。次に、圧縮部113は、コンテンツデータS112を、例えばATRAC3方式で圧縮してコンテンツデータS113を作成し、これを暗号化部114に出力する。また、乱数発生部115から暗号化部114に、乱数を発生して生成されたコンテンツ鍵データK_cが出力される。

【0080】次に、暗号化部114は、コンテンツデータS113と、記憶部119から読み出されたメタデータMetaおよびA/V伸長用ソフトウェアSoftとを、コンテンツ鍵データK_cを用いて暗号化してセキュアコンテナ作成部118に出力する。この場合に、メタデータMetaは暗号化しなくてもよい。そして、セキュアコンテナ作成部118は、図4(A)に示すコンテンツファイルCFを作成する。また、署名処理部117において、コンテンツファイルCFのハッシュ値がとられ、秘密鍵データK_{CP,S}を用いて署名データSIG_{6,CP}が生成される。

【0081】また、署名処理部117は、コンテンツデータC、コンテンツ鍵データK_cおよび権利書データ106のそれぞれに対してハッシュ値をとり、秘密鍵データK_{CP,S}を用いて、それぞれのデータの作成者(提供者)の正当性を示す署名データSIG_{2,CP}、SIG_{3,CP}、SIG_{4,CP}を作成する。また、暗号化部116は、図4(B)に示すコンテンツ鍵データK_c、権利書データ106、SAMプログラム・ダウンロード・コンテナSD₁~SD₃および署名・証明書モジュールMod₁を、対応する期間の配信用鍵データKD₁~KD₃で暗号化してセキュアコンテナ作成部118に出力する。そして、セキュアコンテナ作成部118は、図4(B)に示すキーファイルKFを作成する。また、署名

処理部117は、キーファイルKFのハッシュ値を取り、秘密鍵データK_{CP,S}を用いて、署名データSIG_{7,CP}を作成する。

【0082】次に、セキュアコンテナ作成部118は、図4(A)に示すコンテンツファイルCFおよびその署名データSIG_{6,CP}と、図4(B)に示すキーファイルKFおよびその署名データSIG_{7,CP}と、図4(C)に示す公開鍵証明書データCER_{CP}およびその署名データSIG_{1,ESC}とを格納したセキュアコンテナ104を作成し、これを、セキュアコンテナデータベース118aに記憶する。そして、セキュアコンテナ作成部118は、例えばユーザからの要求(リクエスト)に応じてユーザホームネットワーク103に提供しようとするセキュアコンテナ104をセキュアコンテナデータベース118aから読み出して、相互認証部120とSAM1051との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化・復号部121において暗号化した後に、SAM管理部124を介してユーザホームネットワーク103のSAM1051に送信する。

【0083】次に、コンテンツプロバイダ101が、EMDサービスセンタ102に権利書データ106およびコンテンツ鍵データK_cを登録して権威化することを要求する場合の処理を図3を参照して説明する。権利書データ106およびコンテンツ鍵データK_cの権威化要求処理は、個々のコンテンツデータC毎に行われる。

【0084】この場合には、署名処理部117において、記憶部119から読み出したコンテンツデータCのグローバルユニークな識別子Content_ID、コンテンツ鍵データK_cおよび権利書データ作成部122から入力した権利書データ106からなるモジュールM_{od3}のハッシュ値が求められ、秘密鍵データK_{CP,S}を用いて署名データSIG_{5,CP}が生成される。そして、図6(A)に示す権利登録要求用モジュールM_{od2}を、相互認証部120とEMDサービスセンタ102との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化・復号部121において暗号化した後に、EMDサービスセンタ管理部125からEMDサービスセンタ102に送信する。

【0085】本実施形態では、EMDサービスセンタ102において権利書データ106およびコンテンツ鍵データK_cを権威化した後に、コンテンツプロバイダ101がEMDサービスセンタ102から権威化されたことを証明する権威化証明書モジュールを受信しない場合、すなわちコンテンツプロバイダ101において配信用鍵データKD₁~KD₆を用いて暗号化を行ってキーファイルKFを作成する場合を例示する。但し、本発明は、例えば、EMDサービスセンタ102において権利書データ106およびコンテンツ鍵データK_cを権威化した後に、EMDサービスセンタ102からコンテンツプロバイダ101に、配信用鍵データKD₁~KD₆を用い

て暗号化した図6(B)に示す権威化証明書モジュールM_{od2a}を送信してもよい。権威化証明書モジュールM_{od2a}は、コンテンツデータCのグローバルユニークな識別子Content_ID、コンテンツ鍵データK_cおよび権利書データ作成部122から入力した権利書データ106を格納したモジュールM_{od3a}と、秘密鍵データK_{ESC,S}を用いたモジュールM_{od3a}の署名データSIG_{5a,ESC}とを格納している。この場合には、コンテンツプロバイダ101は、例えば、セキュアコンテナ104内に、権威化証明書モジュールM_{od2a}を格納してSAM1051~1054に配給する。なお、EMDサービスセンタ102は、それぞれ異なる月に対応する配信用鍵データKD₁~KD₆を用いて暗号化した6カ月分の権威化証明書モジュールM_{od2a}を生成し、これらをまとめてコンテンツプロバイダ101に送信してもよい。

【0086】[EMDサービスセンタ102] EMDサービスセンタ102は、認証(CA:Certificate Authority)機能、鍵管理(Key Management)機能および権利処理(Rights Clearing)(利益分配)機能を有する。図7は、EMDサービスセンタ102の機能の構成図である。図7に示すように、EMDサービスセンタ102は、鍵サーバ141、鍵データベース141a、決算処理部142、署名処理部143、決算機関管理部144、証明書・権利書管理部145、CERデータベース145a、コンテンツプロバイダ管理部148、CPデータベース148a、SAM管理部149、SAMデータベース149a、相互認証部150および暗号化・復号部151を有する。なお、図7には、EMDサービスセンタ102内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ101との間で送受信されるデータに関連するデータの流が示されている。また、図8には、EMDサービスセンタ102内の機能ブロック相互間のデータの流のうちの、SAM1051~1054および図1に示す決済機関91との間で送受信されるデータに関連するデータの流が示されている。

【0087】鍵サーバ141は、鍵データベース141aに記憶された各々有効期間が1カ月の配信用鍵データを要求に応じて読み出してコンテンツプロバイダ管理部148およびSAM管理部149に出力する。また、鍵データベース141a配信用鍵データKDの他に、記録用鍵データK_{STR}、メディア鍵データK_{MED}およびMAC鍵データK_{MAC}などの鍵データを記憶する一連の鍵データースからなる。

【0088】決算処理部142は、SAM1051~1054から入力した利用履歴データ108と、証明書・権利書管理部145から入力した標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済レポートデータ107および決済請求権データ152を作成し、決済レポートデータ107をコンテンツプロバ

イダ管理部148に出力し、決済請求権データ152を
決算機関管理部144に出力する。なお、決算処理部1
42は、販売価格に基づいて、違法なダンピング価格に
よる取り引きが行われたか否かを監視する。ここで、利
用履歴データ108は、ユーザホームネットワーク10
3におけるセキュアコンテナ104の購入、利用（再
生、記録および転送など）の履歴を示し、決算処理部1
42においてセキュアコンテナ104に関連したライン
センス料の支払い額を決定する際に用いられる。

【0089】利用履歴データ108には、例えば、セキ
ュアコンテナ104に格納されたコンテンツデータCの
識別子Content_ID、セキュアコンテナ104
を配給したコンテンツプロバイダ101の識別子CP_
ID、セキュアコンテナ104内のコンテンツデータC
の圧縮方法、セキュアコンテナ104を記録した記録媒
体の識別子Media_ID、セキュアコンテナ104
を配給を受けたSAM1051~1054の識別子SA
M_ID、当該SAM1051~1054のユーザのU
SER_IDなどが記述されている。従って、EMDサ
ービスセンタ102は、コンテンツプロバイダ101の
所有者以外にも、例えば、圧縮方法や記録媒体などのラ
イセンス所有者に、ユーザホームネットワーク103の
ユーザが支払った金銭を分配する必要がある場合には、
予め決められた分配率表に基づいて各相手に支払う金額
を決定し、当該決定に応じた決済レポートデータ107
および決済請求権データ152を作成する。当該分配率
表は、例えば、セキュアコンテナ104に格納されたコ
ンテンツデータ毎に作成される。また、決済請求権デー
タ152は、当該データに基づいて、決済機関91に金
銭の支払いを請求できる権威化されたデータであり、例
えば、ユーザが支払った金銭を複数の権利者に配給する
場合には、個々の権利者毎に作成される。なお、決済機
関91は、決済が終了すると、当該決済機関の利用明細
書をEMDサービスセンタ102に送る。EMDサー
ビスセンタ102は、当該利用明細書の内容を、対応する
権利者に通知する。

【0090】決算機関管理部144は、決算処理部14
2が生成した決済請求権データ152を図1に示すペ
イメントゲートウェイ90を介して決済機関91に送信
する。なお、後述するように、決算機関管理部144
は、決済請求権データ152を、コンテンツプロバイダ
101などの権利者に送信し、権利者自らが、受信した
決済請求権データ152を用いて決済機関91に決済を
行ってもよい。また、決算機関管理部144は、署名処
理部143において決済請求権データ152のハッシュ
値を取り、秘密鍵データK_{ESC,S}を用いて生成した署名
データSIG₉₉を決済請求権データ152と共に決済機
関91に送信する。

【0091】証明書・権利書管理部145は、CERデ
ータベース145aに登録されて権威化された公開鍵証

明書データCER_{CP}および公開鍵証明書データCER
SAM1~CER_{SAM4}などを読み出すと共に、コンテンツプ
ロバイダ101の権利書データ106およびコンテン
ツ鍵データK_cなどをCERデータベース145aに登録
して権威化する。なお、公開鍵証明書データCER_{SAM1}
~CER_{SAM4}を格納するデータースと、権利書データ1
06およびコンテンツ鍵データK_cとを個別に設けても
よい。このとき、証明書・権利書管理部145は、例え
ば、権利書データ106およびコンテンツ鍵データK_c
などのハッシュ値を取り、秘密鍵データK_{ESC,S}を用い
た署名データを付した権威化されたそれぞれの証明書デ
ータを作成する。

【0092】コンテンツプロバイダ管理部148は、コ
ンテンツプロバイダ101との間で通信する機能を有
し、登録されたコンテンツプロバイダ101の識別子C
P_IDなどを管理するCPデータベース148aにア
クセスできる。

【0093】SAM管理部149は、ユーザホームネッ
トワーク103内のSAM1051~1054との間で
通信する機能を有し、登録されたSAMの識別子SAM
_IDやSAM登録リストなどを記録したSAMデー
タベース149aにアクセスできる。

【0094】以下、EMDサービスセンタ102内での
処理の流れを説明する。まず、EMDサービスセンタ1
02からコンテンツプロバイダ101およびユーザホ
ムネットワーク103内のSAM1051~1054へ
の配信用鍵データを送信する際の処理の流れを、図7お
よび図8を参照しながら説明する。図7に示すように、
鍵サーバ141は、所定期間毎に、例えば、6カ月分の
配信用鍵データKD₁~KD₆を鍵データベース141
aから読み出してコンテンツプロバイダ管理部148に
出力する。また、署名処理部143は、配信用鍵データ
KD₁~KD₆の各々のハッシュ値を取り、EMDサー
ビスセンタ102の秘密鍵データK_{ESC,S}を用いて、そ
れぞれに対応する署名データSIG_{KD1,ESC}~SIG
KD6,ESCを作成し、これをコンテンツプロバイダ管理部
148に出力する。コンテンツプロバイダ管理部148
は、この6カ月分の配信用鍵データKD₁~KD₆およ
びそれらの署名データSIG_{KD1,ESC}~SIG_{KD6,ESC}
を、相互認証部150と図3に示す相互認証部120と
間の相互認証で得られたセッション鍵データK_{SES}を用
いて暗号化した後に、コンテンツプロバイダ101に送
信する。

【0095】また、図8に示すように、鍵サーバ141
は、所定期間毎に、例えば、3カ月分の配信用鍵デー
タKD₁~KD₃を鍵データベース141aから読み出し
てSAM管理部149に出力する。また、署名処理部1
43は、配信用鍵データKD₁~KD₃の各々のハッシ
ュ値を取り、EMDサービスセンタ102の秘密鍵デー
タK_{ESC,S}を用いて、それぞれに対応する署名データS

51

IGKD1,ESC ~ SIGKD3,ESCを作成し、これをSAM管理部149に出力する。SAM管理部149は、この3カ月分の配信鍵データKD1 ~ KD3 およびそれらの署名データSIGKD1,ESC ~ SIGKD3,ESCを、相互認証部150とSAM1051 ~ 1054と間の相互認証で得られたセッション鍵データKSESを用いて暗号化した後に、SAM1051 ~ 1054に送信する。

【0096】次に、EMDサービスセンタ102がコンテンツプロバイダ101から、公開鍵証明書データCERcpの発行要求を受けた場合の処理を、図7を参照しながら説明する。この場合に、コンテンツプロバイダ管理部148は、コンテンツプロバイダ101の識別子CP_ID、公開鍵データKcp,Pおよび署名データSIG9,CPをコンテンツプロバイダ101から受信すると、これらを、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データKSESを用いて復号する。そして、当該復号した署名データSIG9,CPの正当性を署名処理部143において確認した後に、識別子CP_IDおよび公開鍵データKcp,Pに基づいて、当該公開鍵証明書データの発行要求を出したコンテンツプロバイダ101がCPデータベース148aに登録されているか否かを確認する。そして、証明書・権利書管理部145は、当該コンテンツプロバイダ101の公開鍵証明書データCERcpをCERデータベース145aから読み出してコンテンツプロバイダ管理部148に出力する。また、署名処理部143は、公開鍵証明書データCERcpのハッシュ値をとり、EMDサービスセンタ102の秘密鍵データKESC,Sを用いて、署名データSIG1,ESCを作成し、これをコンテンツプロバイダ管理部148に出力する。そして、コンテンツプロバイダ管理部148は、公開鍵証明書データCERcpおよびその署名データSIG1,ESCを、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データKSESを用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0097】次に、EMDサービスセンタ102がSAM1051から、公開鍵証明書データCERSAM1の発行要求を受けた場合の処理を、図8を参照しながら説明する。この場合に、SAM管理部149は、SAM1051の識別子SAM1_ID、公開鍵データKSAM1,Pおよび署名データSIG8,SAM1をSAM1051から受信すると、これらを、相互認証部150とSAM1051と間の相互認証で得られたセッション鍵データKSESを用いて復号する。そして、当該復号した署名データSIG8,SAM1の正当性を署名処理部143において確認した後に、識別子SAM1_IDおよび公開鍵データKSAM1,Pに基づいて、当該公開鍵証明書データの発行要求を出したSAM1051がSAMデータベース149aに登録されているか否かを確認する。そして、証明書・権利書管理部145は、当該SAM1051の公開鍵証明書デ

52

ータCERSAM1をCERデータベース145aから読み出してSAM管理部149に出力する。た、署名処理部143は、公開鍵証明書データCERSAM1のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データKESC,Sを用いて、署名データSIG50,ESCを作成し、これをSAM管理部149に出力する。そして、SAM管理部149は、公開鍵証明書データCERSAM1およびその署名データSIG50,ESCを、相互認証部150とSAM1051と間の相互認証で得られたセッション鍵データKSESを用いて暗号化した後に、SAM1051に送信する。なお、SAM1052 ~ 1054が、公開鍵証明書データを要求した場合の処理は、対象がSAM1052 ~ 1054に代わるのみで、基本的に上述したSAM1051の場合と同じである。なお、本発明では、EMDサービスセンタ102は、例えば、SAM1051の出荷時に、SAM1051の秘密鍵データKSAM1,Sおよび公開鍵データKSAM1,PをSAM1051の記憶部に記憶する場合には、当該出荷時に、公開鍵データKSAM1,Pの公開鍵証明書データCERSAM1を作成してもよい。このとき、当該出荷時に、公開鍵証明書データCERSAM1を、SAM1051の記憶部に記憶してもよい。

【0098】次に、EMDサービスセンタ102が、コンテンツプロバイダ101から権利書データ106およびコンテンツ鍵データKcの登録要求を受けた場合の処理を、図7を参照しながら説明する。この場合には、コンテンツプロバイダ管理部148がコンテンツプロバイダ101から図6(A)に示す権利書登録要求モジュールMod2を受信すると、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データKSESを用いて権利書登録要求モジュールMod2を復号する。そして、署名処理部143において、鍵データベース141aから読み出した公開鍵データKcpを用いて、署名データSIG5,CPの正当性を検証する。次に、証明書・権利書管理部145は、権利書登録要求モジュールMod2に格納された権利書データ106およびコンテンツ鍵データKcを、CERデータベース145aに登録する。

【0099】次に、EMDサービスセンタ102において決済処理を行なう場合の処理を図8を参照しながら説明する。SAM管理部149は、ユーザホームネットワーク103の例えばSAM1051から利用履歴データ108およびその署名データSIG200,SAM1を入力すると、利用履歴データ108および署名データSIG200,SAM1を、相互認証部150とSAM1051との間の相互認証によって得られたセッション鍵データKSESを用いて復号し、SAM1051の公開鍵データKSAM1による署名データSIG200,SAM1の検証を行なった後に、決算処理部142に出力する。

【0100】そして、決算処理部142は、SAM管理部149から入力した利用履歴データ108と、証明書

・権利書管理部145を介してCERデータベース145aから読み出した権利書データ106に含まれる標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を生成する。決算処理部142は、決済請求権データ152を決算機関管理部144に出力すると共に、決済レポートデータ107をコンテンツプロバイダ管理部148に出力する。

【0101】次に、決算機関管理部144は、決済請求権データ152およびその署名データSIG₉₉を、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図1に示すペイメントゲートウェイ90を介して決済機関91に送信する。これにより、決済請求権データ152に示される金額の金銭が、コンテンツプロバイダ101に支払われる。

【0102】次に、EMDサービスセンタ102がコンテンツプロバイダ101に決済レポートを送信する場合の処理を図7を参照しながら説明する。決算処理部142において決済が行なわれると、前述したように、決算処理部142からコンテンツプロバイダ管理部148に決済レポートデータ107が出力される。決済レポートデータ107は、上述したように、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の内容が記述されている。EMDサービスセンタ102は、決算処理部142から決済レポートデータ107を入力すると、これを、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0103】また、EMDサービスセンタ102は、前述したように、権利書データ106を登録(権威化)した後に、EMDサービスセンタ102からコンテンツプロバイダ101に、図6(B)に示す権威化証明書モジュールMod_{2a}を配信用鍵データKD₁~KD₆で暗号化して送信してもよい。

【0104】また、EMDサービスセンタ102は、その他に、SAM105₁~105₄の出荷時の処理と、SAM登録リストの登録処理とを行なうが、これらの処理については後述する。

【0105】【ユーザホームネットワーク103】ユーザホームネットワーク103は、図1に示すように、ネットワーク機器160₁およびA/V機器160₂~160₄を有している。ネットワーク機器160₁は、SAM105₁を内蔵している。また、A/V機器160₂~160₄は、それぞれSAM105₂~105₄を内蔵している。SAM105₁~105₄の相互間は、例えば、IEEE1394シリアルインタフェースバスなどのバス191を介して接続されている。なお、A/V機器160₂~160₄は、ネットワーク通信機能を有し

ていてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器160₁のネットワーク通信機能を利用してもよい。また、ユーザホームネットワーク103は、ネットワーク機能を有していないAV機器のみを有していてもよい。

【0106】以下、ネットワーク機器160₁について説明する。図9は、ネットワーク機器160₁の構成図である。図9に示すように、ネットワーク機器160₁は、SAM105₁、通信モジュール162、復号・伸長モジュール163、購入・利用形態決定操作部165、ダウンロードメモリ167、再生モジュール169および外部メモリ201を有する。

【0107】SAM105₁~105₄は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ102との間で通信を行う。SAM105₁~105₄は、例えば、EMDサービスセンタ102によって仕様およびバージョンなどが管理され、家庭機器メーカーに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカーは、SAM105₁~105₄のIC(Integrated Circuit)の内部の仕様を知ることはできず、EMDサービスセンタ102が当該ICのインタフェースなどを統一化し、それに従ってネットワーク機器160₁およびAV機器160₂~160₄に搭載される。

【0108】SAM105₁~105₄は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ(Tamper Resistance)性を持ったハードウェアモジュール(ICモジュールなど)である。SAM105₁~105₄の機能をICという形で実現する場合は、IC内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。SAMをICという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をSAMとして定義してもよい。

【0109】以下、SAM105₁の機能について詳細に説明する。なお、SAM105₂~105₄は、SAM105₁と基本的に同じ機能を有している。図10は、SAM105₁の機能の構成図である。なお、図10には、コンテンツプロバイダ101からのセキュアコンテナ104を入力し、セキュアコンテナ104内のキーファイルKFを復号する処理に関連するデータの流れが示されている。図10に示すように、SAM105₁は、相互認証部170、暗号化・復号部171、172、173、コンテンツプロバイダ管理部180、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監

55

視部186、課金処理部187、署名処理部189、SAM管理部190、メディアSAM管理部197、スタック（作業）メモリ200および外部メモリ管理部811を有する。なお、AV機器1602~1604はダウンロードメモリ167を有していないため、SAM1052~1054にはダウンロードメモリ管理部182は存在しない。

【0110】なお、図10に示すSAM1051の所定の機能は、例えば、図示しないCPUにおいて秘密プログラムを実行することによって実現される。また、スタックメモリ200には、以下に示す処理を経て、図11に示すように、利用履歴データ108およびSAM登録リストが記憶される。ここで、外部メモリ201のメモリ空間は、SAM1051の外部（例えば、ホストCPU810）からは見ることはできず、SAM1051のみが外部メモリ201の記憶領域に対してのアクセスを管理できる。外部メモリ201としては、例えば、フラッシュメモリあるいは強誘電体メモリ（FeRAM）などが用いられる。また、スタックメモリ200としては、例えばSARAMが用いられ、図12に示すように、セキュアコンテナ104、コンテンツ鍵データKc、権利書データ（UCP）106、記憶部192のロック鍵データKLoc、コンテンツプロバイダ101の公開鍵証明書CERcp、利用制御状態データ（UCS）166、およびSAMプログラム・ダウンロード・コンテナSDC1~SDC3などが記憶される。

【0111】以下、SAM1051の機能のうち、コンテンツプロバイダ101からのセキュアコンテナ104を入力したときの各機能ブロックの処理内容を図10を参照しながら説明する。

【0112】相互認証部170は、SAM1051がコンテンツプロバイダ101およびEMDサービスセンタ102との間でオンラインでデータを送受信する際に、コンテンツプロバイダ101およびEMDサービスセンタ102との間で相互認証を行ってセッション鍵データ（共有鍵）Ksesを生成し、これを暗号化・復号部171に出力する。セッション鍵データKsesは、相互認証を行う度に新たに生成される。

【0113】暗号化・復号部171は、コンテンツプロバイダ101およびEMDサービスセンタ102との間で送受信するデータを、相互認証部170が生成したセッション鍵データKsesを用いて暗号化・復号する。

【0114】誤り訂正部181は、セキュアコンテナ104を誤り訂正してダウンロードメモリ管理部182に出力する。なお、ユーザホームネットワーク103は、セキュアコンテナ104が改竄されているか否かを検出する機能を有していてもよい。本実施形態では、誤り訂正部181を、SAM1051に内蔵した場合を例示したが、誤り訂正部181の機能を、例えばホストCPU810などのSAM1051の外部に持たせてもよい。

56

【0115】ダウンロードメモリ管理部182は、図9に示すようにダウンロードメモリ167が相互認証機能を持つメディアSAM167aを有している場合には、相互認証部170とメディアSAM167aとの間で相互認証を行った後に、誤り訂正後のセキュアコンテナ104を、相互認証によって得られたセッション鍵データKsesを用いて暗号化して図9に示すダウンロードメモリ167に書き込む。ダウンロードメモリ167としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。なお、図13に示すように、HDD（Hard Disk Drive）などの相互認証機能を備えていないメモリをダウンロードメモリ211として用いる場合には、ダウンロードメモリ211内はセキュアではないので、コンテンツファイルCFをダウンロードメモリ211にダウンロードし、機密性の高いキーファイルKFを例えば、図10に示すスタックメモリ200にダウンロードする。

【0116】セキュアコンテナ復号部183は、ダウンロードメモリ管理部182から入力したセキュアコンテナ104に格納されたキーファイルKFを、記憶部192から読み出した対応する期間の配信用鍵データKD1~KD3を用いて復号し、署名処理部189において署名データSIG2,CP~SIG4,CPの正当性、すなわちコンテンツデータC、コンテンツ鍵データKcおよび権利書データ106の作成者の正当性を確認した後に、スタックメモリ200に書き込む。

【0117】EMDサービスセンタ管理部185は、図1に示すEMDサービスセンタ102との間の通信を管理する。

【0118】署名処理部189は、記憶部192から読み出したEMDサービスセンタ102の公開鍵データKESC,Pおよびコンテンツプロバイダ101の公開鍵データKcp,Pを用いて、セキュアコンテナ104内の署名データの検証を行なう。

【0119】記憶部192は、SAM1051の外部から読み出しおよび書き換えできない秘密データとして、図14に示すように、配信用鍵データKD1~KD3、SAM_ID、ユーザID、パスワード、情報参照ID、SAM登録リスト、記録用鍵データKSTR、ルートCAの公開鍵データKR-CA,P、EMDサービスセンタ102の公開鍵データKESC,P、メディア鍵データKMED、EMDサービスセンタ102の公開鍵データKESC,P、SAM1051の秘密鍵データKSAM1,S、SAM1051の公開鍵データKSAM1,Pを格納した公開鍵証明書CERSAM1、EMDサービスセンタ102の秘密鍵データKESC,Sを用いた公開鍵証明書CERESCの署名データSIG22、復号・伸長モジュール163との間の相互認証用の元鍵データ、メディアSAMとの間の相互認証用の元鍵データを記憶している。また、記憶部192には、図10に示す少なくとも一部の機能を実現する

57

ための秘密プログラムが記憶されている。記憶部 192 としては、例えば、フラッシューEEPROM(Electrically Erasable Programmable RAM)が用いられる。

【0120】以下、EMDサービスセンタ102から受信した配信用鍵データKD₁～KD₃を記憶部192に格納する際のSAM105₁内での処理の流れを図10を参照しながら説明する。この場合には、まず、相互認証部170と図7に示す相互認証部150との間で相互認証が行われる。次に、当該相互認証によって得られたセッション鍵データK_{SES}で暗号化された3カ月分の配信用鍵データKD₁～KD₃およびその署名データSIG_{KD1,ESC}～SIG_{KD3,ESC}が、EMDサービスセンタ102からEMDサービスセンタ管理部185を介してスタックメモリ811に書き込まれる。次に、暗号化・復号部171において、セッション鍵データK_{SES}を用いて、配信用鍵データKD₁～KD₃およびその署名データSIG_{KD1,ESC}～SIG_{KD3,ESC}が復号される。次に、署名処理部189において、スタックメモリ811に記憶された署名データSIG_{KD1,ESC}～SIG_{KD3,ESC}の正当性が確認された後に、配信用鍵データKD₁～KD₃が記憶部192に書き込まれる。

【0121】以下、セキュアコンテナ104をコンテンツプロバイダ101から入力し、セキュアコンテナ104内のキーファイルKFを復号する際のSAM105₁内での処理の流れを図10を参照しながら説明する。図10に示すSAM105₁の相互認証部170と図2に示す相互認証部120との間で相互認証が行なわれる。暗号化・復号部171は、当該相互認証によって得られたセッション鍵データK_{SES}を用いて、コンテンツプロバイダ管理部180を介してコンテンツプロバイダ101から供給されたセキュアコンテナ104を復号する。

【0122】次に、署名処理部189は、図4(C)に示す署名データSIG_{1,ESC}の検証を行なった後に、図4(C)に示す公開鍵証明書データCER_{CP}内に格納されたコンテンツプロバイダ101の公開鍵データK_{CP,P}を用いて、署名データSIG_{6,CP}、SIG_{7,CP}の正当性を確認する。コンテンツプロバイダ管理部180は、署名データSIG_{6,CP}、SIG_{7,CP}の正当性が確認されると、セキュアコンテナ104を誤り訂正部181に出力する。

【0123】誤り訂正部181は、セキュアコンテナ104を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。ダウンロードメモリ管理部182は、相互認証部170と図9に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ104をダウンロードメモリ167に書き込む。

【0124】次に、ダウンロードメモリ管理部182は、相互認証部170と図9に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ104に格納された図4(B)に示すキーファイルK

58

Fをダウンロードメモリ167から読み出してセキュアコンテナ復号部183に出力する。

【0125】そして、セキュアコンテナ復号部183は、記憶部192から入力した対応する期間の配信用鍵データKD₁～KD₃を用いて、キーファイルKFを復号し、図4(B)に示す署名・証明書モジュールMod1に格納された署名データSIG_{1,ESC}、SIG_{2,CP}～SIG_{4,CP}を署名処理部189に出力する。署名処理部189は、図4(B)に示す署名データSIG_{1,ESC}の検証を行なった後に、図4(B)に示す公開鍵証明書データCER_{CP}内に格納された公開鍵データK_{ESC,P}を用いて署名データSIG_{2,CP}～SIG_{4,CP}の検証を行なう。これにより、コンテンツデータC、コンテンツ鍵データK_cおよび権利書データ106の作成者の正当性が検証される。

【0126】次に、セキュアコンテナ復号部183は、署名データSIG_{2,CP}～SIG_{4,CP}の正当性が確認されると、キーファイルKFをスタックメモリ200に書き込む。

【0127】以下、ダウンロードメモリ167にダウンロードされたコンテンツデータCを利用・購入する処理に関連する各機能ブロックの処理内容を図15を参照しながら説明する。

【0128】利用監視部186は、スタックメモリ200から権利書データ106および利用制御状態データ166を読み出し、当該読み出した権利書データ106および利用制御状態データ166によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。ここで、権利書データ106は、図10を用いて説明したように、復号後にスタックメモリ200に記憶された図4(B)に示すキーファイルKF内に格納されている。また、利用制御状態データ166は、後述するように、ユーザによって購入形態が決定されたときに、スタックメモリ200に記憶される。

【0129】課金処理部187は、図9に示す購入・利用形態決定操作部165からの操作信号S165に応じた利用履歴データ108を作成する。ここで、利用履歴データ108は、前述したように、ユーザによるセキュアコンテナ104の購入および利用の形態の履歴を記述しており、EMDサービスセンタ102において、セキュアコンテナ104の購入に応じた決済処理およびライセンス料の支払いを決定する際に用いられる。

【0130】また、課金処理部187は、必要に応じて、スタックメモリ200から読み出した販売価格あるいは標準小売価格データSRPをユーザに通知する。ここで、販売価格および標準小売価格データSRPは、復号後にスタックメモリ200に記憶された図4(B)に示すキーファイルKFの権利書データ106内に格納されている。課金処理部187による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用

59

許諾条件などの権利内容および利用制御状態データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【0131】また、課金処理部187は、操作信号S165に基づいて、ユーザによるコンテンツの購入形態を記述した利用制御状態（UCS: Usage Control Status）データ166を生成し、これをスタックメモリ200書き込む。コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。ここで、利用制御状態データ166は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ166には、コンテンツのID、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれたSAMのSAM_ID、購入を行なったユーザのUSER_IDなどが記述されている。

【0132】なお、決定された購入形態が再生課金である場合には、例えば、SAM105₁からコンテンツプロバイダ101に利用制御状態データ166をコンテンツデータCの購入と同時にリアルタイムに送信し、コンテンツプロバイダ101がEMDサービスセンタ102に、利用履歴データ108を所定の期間内にSAM105₁に取りに行くことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ166が、コンテンツプロバイダ101およびEMDサービスセンタ102の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御状態データ166をコンテンツプロバイダ101にリアルタイムに送信する。

【0133】EMDサービスセンタ管理部185は、外部メモリ管理部811を介して外部メモリ201から読み出した利用履歴データ108をEMDサービスセンタ102に送信する。このとき、EMDサービスセンタ管理部185は、署名処理部189において、秘密鍵データKSAM_{1,s}を用いて利用履歴データ108の署名データSIG_{200,SAM1}を作成し、署名データSIG_{200,SAM1}を利用履歴データ108と共にEMDサービスセンタ102に送信する。EMDサービスセンタ102への利用履歴データ108の送信は、例えば、EMDサービスセンタ102からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ108に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ201の記憶容量に応じて決定される。

【0134】ダウンロードメモリ管理部182は、例えば、図9に示す購入形態決定操作部165からの操作信

60

号S165に応じてコンテンツの再生動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツデータC、スタックメモリ200から読み出したコンテンツ鍵データKcおよび課金処理部187から入力したユーザ電子透かし情報用データ196を復号・伸長モジュール管理部184に出力する。また、復号・伸長モジュール管理部184は、図9に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの試聴動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツファイルCF、並びにスタックメモリ200から読み出したコンテンツ鍵データKcおよび半開示パラメータデータ199を復号・伸長モジュール管理部184に出力する。

【0135】ここで、半開示パラメータデータ199は、権利書データ106内に記述されており、試聴モード時のコンテンツの取り扱いを示している。復号・伸長モジュール163では、半開示パラメータデータ199に基づいて、暗号化されたコンテンツデータCを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、復号・伸長モジュール163がデータ（信号）を所定のブロックを単位として処理することを利用して、半開示パラメータデータ199によって、コンテンツ鍵データKcを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

【0136】以下、SAM105₁内での処理の流れについて説明する。まず、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテナ104の購入形態を決定するまでの処理の流れを図15を参照しながら説明する。まず、ユーザによる図9に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が課金処理部187に出力されると、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図9に示す復号・伸長モジュール163に出力される。このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データK_{SES}による暗号化・復号とが行なわれる。コンテンツファイルCFは、図9に示す復号部221において復号された後に、復号部222に出力される。

【0137】また、スタックメモリ200から読み出されたコンテンツ鍵データKcおよび半開示パラメータデータ199が、図9に示す復号・伸長モジュール163に出力される。このとき、相互認証部170と相互認証部220との間の相互認証後に、コンテンツ鍵データK

61

cおよび半開示パラメータデータ199に対してセッション鍵データKsesによる暗号化および復号が行なわれる。次に、復号された半開示パラメータデータ199が半開示処理部225に出力され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データKcを用いたコンテンツデータCの復号が半開示で行われる。次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長された後に、電子透かし情報処理部224に出力される。次に、電子透かし情報処理部224においてユーザ電子透かし情報用データ196がコンテンツデータCに埋め込まれた後、コンテンツデータCが再生モジュール169において再生され、コンテンツデータCに応じた音響が出力される。

【0138】そして、コンテンツを試聴したユーザが、購入・利用形態決定操作部165を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号S165が課金処理部187に出力される。そして、課金処理部187において、決定された購入形態に応じた利用履歴データ108および利用制御状態データ166が生成され、利用履歴データ108が外部メモリ管理部811を介して外部メモリ201に書き込まれると共に、利用制御状態データ166がスタックメモリ200に書き込まれる。以後は、利用監視部186において、利用制御状態データ166によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。そして、スタックメモリ200に格納されているキーファイルKFに、利用制御状態データ166が加えられ、購入形態が決定した後述する図18（B）に示す新たなキーファイルKF₁が生成される。キーファイルKF₁は、スタックメモリ200に記憶される。図18（B）に示すように、キーファイルKF₁に格納された利用制御状態データ166はストレージ鍵データKSTRを用いてDESのCBCモードを利用して暗号化されている。また、当該ストレージ鍵データKSTRをMAC（Message Authentication Code）鍵データとして用いて生成したMAC値であるMAC₃₀₀が付されている。また、利用制御状態データ166およびMAC₃₀₀からなるモジュールは、メディア鍵データKMEDを用いてDESのCBCモードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データKMEDをMAC鍵データとして用いて生成したMAC値であるMAC₃₀₁が付されている。

【0139】次に、ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCを再生する場合の処理の流れを、図15を参照しながら説明する。この場合には、利用監視部186の監視下で、操作信号S165に基づいて、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、図9に示す復号・伸長モジュール163に出力される。このとき、図15に示す相互認証部170と、図9に示す

62

復号・伸長モジュール163の相互認証部220との間で相互認証が行われる。また、スタックメモリ200から読み出されたコンテンツ鍵データKcが復号・伸長モジュール163に出力される。そして、復号・伸長モジュール163の復号部222において、コンテンツ鍵データKcを用いたコンテンツファイルCFの復号と、伸長部223による伸長処理とが行なわれ、再生モジュール169において、コンテンツデータCが再生される。このとき、課金処理部187によって、操作信号S165に応じて、外部メモリ201に記憶されている利用履歴データ108が更新される。利用履歴データ108は、外部メモリ201から読み出された後、相互認証を経て、EMDサービスセンタ管理部185を介して、署名データSIG₂₀₀,SAM₁と共にEMDサービスセンタ102に送信される。

【0140】次に、図16に示すように、例えば、ネットワーク機器160₁のダウンロードメモリ167にダウンロードされた既に購入形態が決定されたコンテンツファイルCFおよびキーファイルKFを、バス191を介して、AV機器160₂のSAM105₂に転送する場合のSAM105₁内での処理の流れを図17を参照しながら説明する。ユーザは、購入・利用形態決定操作部165を操作して、ダウンロードメモリ167に記憶された所定のコンテンツをAV機器160₂に転送することを指示し、当該操作に応じた操作信号S165が、課金処理部187に出力される。これにより、課金処理部187は、操作信号S165に基づいて、外部メモリ201に記憶されている利用履歴データ108を更新する。

【0141】また、ダウンロードメモリ管理部182は、ダウンロードメモリ167から読み出した図18（A）に示すコンテンツファイルCFをSAM管理部190に出力する。また、スタックメモリ200から読み出した図18（B）に示すキーファイルKF₁を、署名処理部189およびSAM管理部190に出力する。署名処理部189は、スタックメモリ200から読み出したキーファイルKF₁の署名データSIG₄₂,SAM₁を作成し、これをSAM管理部190に出力する。また、SAM管理部190は、記憶部192から、図18（C）に示す公開鍵証明書データCERSAM₁およびその署名データSIG₂₂,ESCを読み出す。

【0142】また、相互認証部170は、SAM105₂との間で相互認証を行って得たセッション鍵データKsesを暗号化・復号部171に出力する。SAM管理部190は、図18（A）、（B）、（C）に示すデータからなる新たなセキュアコンテンツを購入、暗号化・復号部171において、セッション鍵データKsesを用いて暗号化した後に、図16に示すAV機器160₂のSAM105₂に出力する。このとき、SAM105₁とSAM105₂との間の相互認証と並行して、IEEE1

394 シリアルバスであるバス191の相互認証が行われる。

【0143】以下、図16に示すように、SAM1051から入力したコンテンツファイルCFなどを、RAM型などの記録媒体（メディア）に書き込む際のSAM1052内での処理の流れを、図19を参照しながら説明する。

【0144】この場合には、SAM1052のSAM管理部190は、図16に示すように、図18（A）に示すコンテンツファイルCFと、図18（B）に示すキーファイルKF₁およびその署名データSIG_{42,SAM1}と、図18（C）に示す公開鍵署名データCER_{SAM1}およびその署名データSIG_{22,ESC}とを、ネットワーク機器1601のSAM1051から入力する。そして、暗号化・復号部171において、SAM管理部190が入力したコンテンツファイルCFと、キーファイルKF₁およびその署名データSIG_{42,SAM1}と、公開鍵署名データCER_{SAM1}およびその署名データSIG_{22,ESC}とが、相互認証部170とSAM1051の相互認証部170との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号される。

【0145】次に、セッション鍵データK_{SES}を用いて復号されたキーファイルKF₁およびその署名データSIG_{42,SAM1}と、公開鍵署名データCER_{SAM1}およびその署名データSIG_{22,ESC}とが、スタックメモリ200に書き込まれる。

【0146】次に、署名処理部189は、スタックメモリ200から読み出した署名データSIG_{22,ESC}を、記憶部192から読み出した公開鍵データK_{ESC,P}を用いて検証して、公開鍵証明書データCER_{SAM1}の正当性を確認する。そして、署名処理部189は、公開鍵証明書データCER_{SAM1}の正当性を確認すると、公開鍵証明書データCER_{SAM1}に格納された公開鍵データK_{SAM1,P}を用いて、署名データSIG_{42,SAM1}の正当を確認する。

【0147】次に、署名データSIG_{42,SAM1}の正当性、すなわちキーファイルKF₁の作成者の正当性が確認されると、図18（B）に示すキーファイルKF₁をスタックメモリ200から読み出して暗号化・復号部173に出力する。なお、当該例では、キーファイルKF₁の作成者と送信元とが同じ場合を述べたが、キーファイルKF₁の作成者と送信元とが異なる場合には、キーファイルKF₁に対して作成者の署名データと送信者と署名データとが作成され、署名処理部189において、双方の署名データの正当性が検証される。

【0048】そして、暗号化・復号部173は、記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を用いてキーファイルKF₁を順に暗号化してメディアSAM管理部197に出力する。なお、メディア鍵データK_{MED}は、図17に示す相互認証部170と図16に示す

RAM型の記録媒体250のメディアSAM252との間の相互認証によって記憶部192に事前に記憶されている。

【0149】ここで、記録用鍵データK_{STR}は、例えばSACD(Super Audio Compact Disk)、DVD(Digital Versatile Disc)機器、CD-R機器およびMD(Mini Disc)機器などの種類（当該例では、AV機器1602）に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。なお、SACDとDVDとは、ディスク媒体の物理的な構造が同じであるため、DVD機器を用いてSACDの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データK_{STR}は、このような場合において、不正コピーを防止する役割を果たす。

【0150】また、メディア鍵データK_{MED}は、記録媒体（当該例では、RAM型の記録媒体250）にユニークなデータである。メディア鍵データK_{MED}は、記録媒体（当該例では、図16に示すRAM型の記録媒体250）側に格納されており、記録媒体のメディアSAMにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データK_{MED}は、記録媒体にメディアSAMが搭載されている場合には、当該メディアSAM内に記憶されており、記録媒体にメディアSAMが搭載されていない場合には、例えば、RAM領域内のホストCPU810の管理外の領域に記憶されている。なお、本実施形態のように、機器側のSAM（当該例では、SAM1052）とメディアSAM（当該例では、メディアSAM252）との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データK_{MED}を機器側のSAMに転送し、機器側のSAMにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行なってもよい。本実施形態では、記録用鍵データK_{STR}およびメディア鍵データK_{MED}が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

【0151】また、購入者鍵データK_{PIN}は、コンテンツファイルCFの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してEMDサービスセンタ102によって割り当てられる。購入者鍵データK_{PIN}は、EMDサービスセンタ102において管理される。

【0152】メディアSAM管理部197は、SAM管理部190から入力したコンテンツファイルCFおよび暗号化・復号部173から入力したキーファイルKF₁を、図16に示す記録モジュール260に出力する。そして、記録モジュール260は、メディアSAM管理部197から入力したコンテンツファイルCFおよびキーファイルKF₁を、図16に示すRAM型の記録媒体250のRAM領域251に書き込む。この場合に、キーファイルKF₁を、メディアSAM252内に書き込む

ようにしてもよい。

【0153】次に、コンテンツの購入形態が未決定の図5に示すROM型の記録媒体130をユーザホームネットワーク303がオフラインで配給を受けた場合に、AV機器1602において購入形態を決定する際の処理の流れを図20および図21を参照しながら説明する。AV機器1602のSAM1052は、先ず、図21に示す相互認証部170と図5に示すROM型の記録媒体130のメディアSAM133との間で相互認証を行った後に、メディアSAM133からメディア鍵データK

MEDを入力する。なお、SAM1052が、事前にメディア鍵データK_{MED}を保持している場合には、当該入力を行わなくても良い。次に、ROM型の記録媒体130のRAM領域132に記録されているセキュアコンテナ104に格納された図4(B)、(C)に示すキーファイルKFおよびその署名データSIG_{7,CP}と、公開鍵証明書データCER_{CP}およびその署名データSIG_{1,ESC}とを、メディアSAM管理部197を介して入力し、これをスタックメモリ200に書き込む。

【0154】次に、署名処理部189において、署名データSIG_{1,ESC}の正当性を確認した後に、公開鍵証明書データCER_{CP}から公開鍵データK_{CP,P}を取り出し、この公開鍵データK_{CP,P}を用いて、署名データSIG_{7,CP}の正当性、すなわちキーファイルKFの作成者の正当性を検証する。

【0155】署名処理部189において署名データSIG_{7,CP}の正当性が確認されると、スタックメモリ200からセキュアコンテナ復号部183に、キーファイルKFを読み出す。次に、セキュアコンテナ復号部183において、対応する期間の配信用鍵データKD₁~KD₃を用いて、キーファイルKFを復号する。次に、署名処理部189において、公開鍵データK_{ESC,P}を用いて、キーファイルKFに格納された署名データSIG_{1,ESCM}の正当性を確認した後に、キーファイルKF内の公開鍵証明書データCER_{CP}に格納された公開鍵データK_{CP,P}を用いて、署名データSIG_{2,CP}~SIG_{4,CP}の正当性、すなわちコンテンツデータC、コンテンツ鍵データK_cおよび権利書データ106の作成者の正当性を検証する。

【0156】次に、図21に示す相互認証部170と図20に示す復号・伸長モジュール163との間で相互認証を行った後に、SAM1052の復号・伸長モジュール管理部184は、スタックメモリ200に記憶されているコンテンツ鍵データK_cおよび権利書データ106に格納された半開示パラメータデータ199、並びにROM型の記録媒体130のROM領域131から読み出したコンテンツデータCを図20に示す復号・伸長モジュール163に出力する。次に、復号・伸長モジュール163において、コンテンツデータCがコンテンツ鍵データK_cを用いて半開示モードで復号された後に伸長さ

れ、再生モジュール270に出力される。そして、再生モジュール270において、復号・伸長モジュール163からのコンテンツデータCが再生される。

【0157】次に、ユーザによる図20に示す購入形態決定操作部165の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す操作信号S165が課金処理部187に入力される。

【0158】次に、課金58部187は、操作信号S165に応じた利用制御状態データ166を作成し、これをスタックメモリ200に書き込む。次に、スタックメモリ200から暗号化・復号部173に、例えば、図4(B)に示すキーファイルKFに利用制御状態データ166を格納した図18(B)に示す新たなキーファイルKF₁が出力される。

【0159】次に、暗号化・復号部173は、スタックメモリ200から読み出した図18(B)に示すキーファイルKF₁を、記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を用いて順次に暗号化してメディアSAM管理部197に出力する。次に、図21に示す相互認証部170と図20に示すメディアSAM133との間で相互認証を行った後に、SAM管理部197は、暗号化・復号部173から入力したキーファイルKF₁を図20に示す記録モジュール271を介してROM型の記録媒体130のRAM領域132あるいはメディアSAM133内に書き込む。これにより、購入形態が決定されたROM型の記録媒体130が得られる。このとき、課金処理部187が生成した利用制御状態データ166および利用履歴データ108は、所定のタイミングで、スタックメモリ200および外部メモリ201からそれぞれ読み出しされたEMDサービスセンタ102に送信される。

【0160】以下、図22に示すように、AV機器1603において購入形態が未決定のROM型の記録媒体130からセキュアコンテナ104を読み出してAV機器1602に転送し、AV機器1602において購入形態を決定してRAM型の記録媒体250に書き込む際の処理の流れを説明する。なお、ROM型の記録媒体130からRAM型の記録媒体250へのセキュアコンテナ104の転送は、図1に示すネットワーク機器1601およびAV機器1601~1604のいずれの間で行ってもよい。

【0161】先ず、AV機器1603のSAM1053とROM型の記録媒体130のメディアSAM133との間で相互認証を行い、ROM型の記録媒体130のメディア鍵データK_{MED1}をSAM1053に転送する。また、AV機器1602のSAM1052とRAM型の記録媒体250のメディアSAM252との間で相互認証を行い、RAM型の記録媒体250のメディア鍵データK_{MED2}をSAM1052に転送する。

67

【0162】次に、SAM1053は、ROM型の記録媒体130のROM領域131から読み出した図4

(A)に示すコンテンツファイルCFと、RAM領域132から読み出した図4(B)，(C)キーファイルKF、署名データSIG7、CP、公開鍵証明書データCERCPおよびその署名データSIG1、ESCとを、図23に示す暗号化・復号部172において、対応する期間の配信用鍵データKD1～KD3を用いて順に復号する。次に、暗号化・復号部172で復号されたコンテンツファイルCFは、暗号化・復号部171に出力され、SAM1053と1052との間の相互認証によって得られたセッション鍵データKSESを用いて暗号化された後に、SAM管理部190に出力される。また、暗号化・復号部172で復号されたキーファイルKFは、暗号化・復号部171および署名処理部189に出力される。署名処理部189は、SAM1053の秘密鍵データK350、SAM3を用いて、キーファイルKFの署名データSIG350、SAM3を作成し、これを暗号化・復号部171に出力する。

【0163】また、暗号化・復号部171は、記憶部192から読み出したSAM1053の公開鍵証明書データCER350およびその署名データSIG351、ESCと、キーファイルKFおよびその署名データSIG350、SAM3と、暗号化・復号部172から入力したコンテンツファイルCFとを、SAM1053と1052との間の相互認証によって得られたセッション鍵データKSESを用いて暗号化した後に、SAM管理部190を介して、AV機器1602のSAM1052に出力する。

【0164】SAM1052では、図24に示すように、SAM管理部190を介してSAM1053から入力されたコンテンツファイルCFが、暗号化・復号部171においてセッション鍵データKSESを用いて復号された後に、メディアSAM管理部197を介してRAM型の記録媒体250のRAM領域251に書き込まれる。

【0165】また、SAM管理部190を介してSAM1053から入力されたキーファイルKFおよびその署名データSIG350、SAM3と、公開鍵証明書データCER350およびその署名データSIG351、ESCとが、スタックメモリ200に書き込まれた後に、暗号化・復号部171においてセッション鍵データKSESを用いて復号される。次に、当該復号された署名データSIG351、ESCが、署名処理部189において署名検証され、その正当性が確認されると、公開鍵証明書データCER350に格納された公開鍵データK350を用いて、署名データSIG350、SAM3の正当性が確認されると、スタックメモリ200からキーファイルKFが読み出されてセキュアコンテンツ復号部183に出力される。

68

【0166】次に、セキュアコンテンツ復号部183は、対応する期間の配信用鍵データKD1～KD3を用いて、キーファイルKFを復号し、所定の署名検証を経た後に、当該復号したキーファイルKFをスタックメモリ200に書き込む。

【0167】次に、スタックメモリ200に記憶されている既に復号されたキーファイルKFに格納された権利書データ106が、利用監視部186に出力される。利用監視部186は、権利書データ106に基づいて、コンテンツの購入形態および利用形態が管理される。

【0168】次に、例えば、ユーザによって試聴モードが選択されると、既にセッション鍵データKSESで復号されたコンテンツファイルCFのコンテンツデータCと、スタックメモリ200に記憶されたコンテンツ鍵データKc、権利書データ106から得られた半開示パラメータデータ199およびユーザ電子透かし情報用データ196とが、相互認証を経た後に、図22に示す復号・伸長モジュール管理部184を介して再生モジュール270に出力される。そして、再生モジュール270において、試聴モードに対応したコンテンツデータCの再生が行われる。

【0169】次に、ユーザによる図22に示す購入・利用形態決定操作部165の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作信号S165が、課金処理部187に出力される。そして、課金処理部187において、決定された購入・利用形態に応じて利用制御状態データ166および利用履歴データ108が生成され、これがスタックメモリ200および外部メモリ201にそれぞれ書き込まれる。次に、利用制御状態データ166を格納した例えば図18(B)に示すキーファイルKF1が、スタックメモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において記憶部192から読み出した記録用鍵データKSTR、メディア鍵データKMD2および購入者鍵データKPINを用いて順に暗号化され、メディアSAM管理部197に出力される。キーファイルKF1は、図22に示す記録モジュール271によってRAM型の記録媒体250のRAM領域251あるいはメディアSAM252に書き込まれる。また、利用制御状態データ166および利用履歴データ108は、所定のタイミングで、EMDサービスセンタ102に送信される。

【0170】以下、SAM1051～1054の実現方法について説明する。SAM1051～1054の機能をハードウェアとして実現する場合は、メモリを内蔵したASIC型のCPUを用いて、そのメモリには、図10に示す各機能を実現するためのセキュリティ機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリーモジュール(公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数)、コンテ

ソツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【0171】例えば、図10に示す暗号化・復号部171などのモジュールは、例えば、処理速度の問題でハードウェアとしてASIC型のCPU内のIPコアとして実装される。クロック速度やCPUコード体系などの性能によっては、暗号化・復号部171をソフトウェアとして実装してもよい。また、図10に示す記憶部192や、図10に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリ（フラッシュROM）が用いられ、作業用メモリとしてはSRAMなどの高速書き込み可能なメモリが用いられる。なお、その他にも、SAM1051~1054に内蔵されるメモリとして、強誘電体メモリ（FeRAM）を用いてもよい。また、SAM1051~1054には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

【0172】上述したように、SAM1051~1054は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。SAM1051~1054を搭載した機器のホストCPUのバス経由で、当該SAMのIC内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、SAMのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストCPUが割り付けているアドレス空間内に存在しないように、当該SAMでは、CPU側のメモリー空間を管理するMMU(Memory Magagement Unit)を用いて、搭載機器側のホストCPUからは見えないアドレス空間を設定する。また、SAM1051~1054は、X線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール（ハードウェアICE、ソフトウェアICE）などを用いたりリアルタイムデバッグ（リバースエンジニアリング）が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがIC製造後には使用できないような構造をしている。SAM1051~1054自身は、ハードウェア的な構造においては、メモリを内蔵した通常のASIC型のCPUであり、機能は当該CPUを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なASIC型のCPUと異なる。

【0173】SAM1051~1054の機能を全てソフトウェアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウェア処理をおこなう場合

と、通常のセットに搭載されているホストCPU上のソフトウェア処理で行い、当該処理のときのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがIPコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ICE（デバグ）で実行状況を解読されても、そのタスクの実行順序がバラバラであったり（この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う）、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ（Mini OS）と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

【0174】次に、図9に示す復号・伸長モジュール163について説明する。図9に示すように、復号・伸長モジュール163は、相互認証部220、復号部221、復号部222、伸長部223、電子透かし情報処理部224および半開示処理部225を有する。相互認証部220は、復号・伸長モジュール163がSAM1051からデータを入力する際に、図16に示す相互認証部170との間で相互認証を行ってセッション鍵データKSESを生成する。

【0175】復号部221は、SAM1051から入力したコンテンツ鍵データKc、半開示パラメータデータ199、ユーザ電子透かし情報用データ196およびコンテンツデータCを、セッション鍵データKSESを用いて復号する。そして、復号部221は、復号したコンテンツ鍵データKcおよびコンテンツデータCを復号部222に出力し、復号したユーザ電子透かし情報用データ196を電子透かし情報処理部224に出力し、半開示パラメータデータ199を半開示処理部225に出力する。

【0176】復号部222は、半開示処理部225からの制御に基づいて、コンテンツ鍵データKcを用いて、コンテンツデータCを半開示状態で復号し、復号したコンテンツデータCを伸長部223に出力する。

【0177】伸長部223は、復号されたコンテンツデータCを伸長して、電子透かし情報処理部224に出力する。伸長部223は、例えば、図4(A)に示すコンテンツファイルCFに格納されたA/V伸長用ソフトウェアを用いて伸長処理を行い、例えば、ATRAC3方式で伸長処理を行う。

【0178】電子透かし情報処理部224は、復号されたユーザ電子透かし情報用データ196に応じたユーザ電子透かし情報を、復号されたコンテンツデータCに埋め込み、新たなコンテンツデータCを生成する。電子透かし情報処理部224は、当該新たなコンテンツデータ

Cを再生モジュール169に出力する。このように、ユーザ電子透かし情報は、コンテンツデータCを再生するときに、復号・伸長モジュール163において埋め込まれる。なお、本発明では、コンテンツデータCにユーザ電子透かし情報用データ196を埋め込まないようにしてもよい。

【0179】半開示処理部225は、半開示パラメータデータ199に基づいて、例えば、コンテンツデータCのうち復号を行わないブロックと、復号を行うブロックとを復号部222に指示する。また、半開示処理部225は、その他に、半開示パラメータデータ199に基づいて、試聴時の再生機能を限定したり、試聴可能な期間を限定するなどの制御を行う。

【0180】再生モジュール169は、復号および伸長されたコンテンツデータCに応じた再生を行う。

【0181】次に、コンテンツプロバイダ101、EMDサービスセンタ102およびユーザホームネットワーク103の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを送受信する際のデータフォーマットについて説明する。図25

(A)は、コンテンツプロバイダ101からSAM1051にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ101からSAM1051に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データKSESで暗号化したモジュールMod50が送信される。モジュールMod50には、モジュールMod51およびその秘密鍵データKCP,Sによる署名データSIGCPが格納されている。モジュールMod51には、コンテンツプロバイダ101の秘密鍵データKCP,Pを格納した公開鍵証明書データCERCPと、公開鍵証明書データCERCPに対しての秘密鍵データKESC,Sによる署名データSIGESCと、送信するデータDataとが格納されている。このように、公開鍵証明書データCERCPを格納したモジュールMod50を、コンテンツプロバイダ101からSAM1051に送信することで、SAM1051において署名データSIGCPの検証を行なう際に、EMDサービスセンタ102からSAM1051に公開鍵証明書データCERCPを送信する必要がなくなる。

【0182】図25(B),(C)は、コンテンツプロバイダ101からSAM1051にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ101からSAM1051に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データKSESで暗号化した図25(B)に示すモジュールMod52が送信される。モジュールMod52には、送信するデータDataと、その秘密鍵データKCP,Sによる署名データSIGCPとが

格納されている。また、EMDサービスセンタ102からSAM1051には、EMDサービスセンタ102とSAM1051との間の相互認証によって得たセッション鍵データKSESで暗号化した図25(C)に示すモジュールMod53が送信される。モジュールMod53には、コンテンツプロバイダ101の公開鍵証明書データCERCPと、その秘密鍵データKESC,Sによる署名データSIGESCとが格納されている。

【0183】図25(D)は、SAM1051からコンテンツプロバイダ101にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、SAM1051からコンテンツプロバイダ101に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データKSESで暗号化したモジュールMod54が送信される。モジュールMod54には、モジュールMod55およびその秘密鍵データKSAM1,Sによる署名データSIGSAM1が格納されている。モジュールMod55には、SAM1051の秘密鍵データKSAM1,Pを格納した公開鍵証明書データCERSAM1と、公開鍵証明書データCERSAM1に対しての秘密鍵データKESC,Sによる署名データSIGESCと、送信するデータDataとが格納されている。このように、公開鍵証明書データCERSAM1を格納したモジュールMod55を、SAM1051からコンテンツプロバイダ101に送信することで、コンテンツプロバイダ101において署名データSIGSAM1の検証を行なう際に、EMDサービスセンタ102からコンテンツプロバイダ101に公開鍵証明書データCERSAM1を送信する必要がなくなる。

【0184】図25(E),(F)は、SAM1051からコンテンツプロバイダ101にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、SAM1051からコンテンツプロバイダ101に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データKSESで暗号化した図25(E)に示すモジュールMod56が送信される。モジュールMod56には、送信するデータDataと、その秘密鍵データKSAM1,Sによる署名データSIGSAM1とが格納されている。また、EMDサービスセンタ102からコンテンツプロバイダ101には、EMDサービスセンタ102とコンテンツプロバイダ101との間の相互認証によって得たセッション鍵データKSESで暗号化した図25(F)に示すモジュールMod57が送信される。モジュールMod57には、SAM1051の公開鍵証明書データCERSAM1と、その秘密鍵データKESC,Sによる署名データSIGESCとが格納されている。

【0185】図26(G)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータData

73

をイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールMod58が送信される。モジュールMod58には、モジュールMod59およびその秘密鍵データK_{CP,S}による署名データSIG_{CP}が格納されている。モジュールMod59には、コンテンツプロバイダ101の秘密鍵データK_{CP,P}を格納した公開鍵証明書データCER_{CP}と、公開鍵証明書データCER_{CP}に対しての秘密鍵データK_{ESC,S}による署名データSIG_{ESC}と、送信するデータDataとが格納されている。

【0186】図26(H)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図26(H)に示すモジュールMod60が送信される。モジュールMod60には、送信するデータDataと、その秘密鍵データK_{CP,S}による署名データSIG_{CP}とが格納されている。このとき、EMDサービスセンタ102にはコンテンツプロバイダ101の公開鍵証明書データCER_{CP}は既に登録されている。

【0187】図26(I)は、SAM1051からEMDサービスセンタ102にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、SAM1051からEMDサービスセンタ102に、EMDサービスセンタ102とSAM1051との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールMod61が送信される。モジュールMod61には、モジュールMod62およびその秘密鍵データK_{SAM1,S}による署名データSIG_{SAM1}が格納されている。モジュールMod62には、SAM1051の秘密鍵データK_{SAM1,P}を格納した公開鍵証明書データCER_{SAM1}と、公開鍵証明書データCER_{SAM1}に対しての秘密鍵データK_{ESC,S}による署名データSIG_{ESC}と、送信するデータDataとが格納されている。

【0188】図26(J)は、SAM1051からEMDサービスセンタ102にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、SAM1051からEMDサービスセンタ102に、EMDサービスセンタ102とSAM1051との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図26

74

(J)に示すモジュールMod63が送信される。モジュールMod63には、送信するデータDataと、その秘密鍵データK_{SAM1,S}による署名データSIG_{SAM1}とが格納されている。このとき、EMDサービスセンタ102にはSAM1051の公開鍵証明書データCER_{SAM1}は既に登録されている。以下、SAM1051~1054の出荷時におけるEMDサービスセンタ102への登録処理について説明する。なお、SAM1051~1054の登録処理は同じであるため、以下、SAM1051の登録処理について述べる。SAM1051の出荷時には、図8に示すEMDサービスセンタ102の鍵サーバ141によって、SAM管理部149を介して、図10などに示す記憶部192に以下に示す鍵データが初期登録される。また、SAM1051には、例えば、出荷時に、記憶部192などに、SAM1051がEMDサービスセンタ102に初回にアクセスする際に用いられるプログラムなどが記憶される。すなわち、記憶部192には、例えば、図14において左側に「*」が付されているSAM1051の識別子SAM_ID、記録用鍵データK_{STR}、ルート認証局2の公開鍵データK_{R-CA}、EMDサービスセンタ102の公開鍵データK_{ESC,P}、SAM1051の秘密鍵データK_{SAM1,S}、公開鍵証明書データCER_{SAM1}およびその署名データSIG_{22,ESC}、復号・伸長モジュール163およびメディアSAMとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。なお、公開鍵証明書データCER_{SAM1}は、SAM1051を出荷後に登録する際にEMDサービスセンタ102からSAM1051に送信してもよい。

【0189】ここで、ルート認証局2の公開鍵データK_{R-CA}は、インターネットの電子商取引などでは一般的に使用されているRSAを使用し、データ長は例えば1024ビットである。公開鍵データK_{R-CA}は、図1に示すルート認証局2によって発行される。また、EMDサービスセンタ102の公開鍵データK_{ESC,P}は、短いデータ長でRSAと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば160ビットである。但し、暗号化の強度を考慮すると、公開鍵データK_{ESC,P}は192ビット以上であることが望ましい。また、EMDサービスセンタ102は、ルート認証局92に公開鍵データK_{ESC,P}を登録する。また、ルート認証局92は、公開鍵データK_{ESC,P}の公開鍵証明書データCER_{ESC}を作成する。公開鍵データK_{ESC,P}を格納した公開鍵証明書データCER_{ESC}は、好ましく、SAM1051の出荷時に記憶部192に記憶される。この場合に、公開鍵証明書データCER_{ESC}は、ルート認証局92の秘密鍵データK_{ROOT,S}で署名されている。

【0190】EMDサービスセンタ102は、乱数を発生してSAM1051の秘密鍵データK_{SAM1,S}を生成

し、これとペアとなる公開鍵データK_{SAM1,P}を生成する。また、EMDサービスセンタ102は、ルート認証局92の認証をもらって、公開鍵データK_{SAM1,P}の公開鍵証明書データCER_{SAM1}を発行し、これに自らの秘密鍵データK_{ESC,S}を用いて署名データを添付する。すなわち、EMDサービスセンタ102は、セカンドCA（認証局）として機能を果たす。

【0191】また、SAM1051には、図8に示すEMDサービスセンタ102のSAM管理部149により、EMDサービスセンタ102の管理下にある一意（ユニーク）な識別子SAM_IDが割り当てられ、これがSAM1051の記憶部192に格納されると共に、図8に示すSAMデータベース149aにも格納され、EMDサービスセンタ102によって管理される。

【0192】また、SAM1051は、出荷後、例えば、ユーザによってEMDサービスセンタ102と接続され、登録手続を行うと共に、EMDサービスセンタ102から記憶部192に配信用鍵データKD₁～KD₃が転送される。すなわち、SAM1051を利用するユーザは、コンテンツをダウンロードする前にEMDサービスセンタ102に登録手続が必要である。この登録手続は、例えば、SAM1051を搭載している機器（当該例では、ネットワーク機器1601）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報を記載して例えば郵便などのオフラインで行なわれる。SAM1051は、上述した登録手続を経た後でないと使用できない。

【0193】EMDサービスセンタ102は、SAM1051のユーザによる登録手続に応じて、ユーザに固有の識別子USER_IDを発行し、例えば、図8に示すSAMデータベース149aにおいて、SAM_IDとUSER_IDとの対応関係を管理し、課金時に利用する。また、EMDサービスセンタ102は、SAM1051のユーザに対して情報参照用識別子IDと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子IDとパスワードとを用いて、EMDサービスセンタ102に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。また、EMDサービスセンタ102は、ユーザの登録時に、クレジットカード会社などに身分の確認を行ったり、オフラインで本人の確認を行なう。

【0194】次に、図14に示すように、SAM1051内の記憶部192にSAM登録リストを格納する手順について説明する。図1に示すSAM1051は、例えば、バス191としてIEEE1394シリアルバスを用いた場合に、バス191に接続された機器の電源を立ち上げたり、新しい機器をバス191に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するSAM1052～SAM1054のSAM登録リ

ストを得る。なお、IEEE1394シリアルバスであるバス191に応じて生成されたトポロジーマップは、例えば、図27に示すように、バス191にSAM1051～1054に加えてAV機器1605, 1606のSCMS処理回路1055, 1056が接続されている場合に、SAM1051～1054およびSCMS処理回路1055, 1056を対象として生成される。従って、SAM1051は、当該トポロジーマップから、SAM1051～1054についての情報を抽出してSAM登録リストを生成する。

【0195】SAM登録リストのデータフォーマットは、例えば、図28に示される。そして、SAM1051は、当該SAM登録リストを、EMDサービスセンタ102に登録して署名を得る。これらの処理は、バス191のセッションを利用してSAM1051が自動的に行い、EMDサービスセンタ102にSAM登録リストの登録命令を発行する。EMDサービスセンタ102は、SAM1051から図28に示すSAM登録リストを受けると、有効期限を確認する。そして、EMDサービスセンタ102は、登録時にSAM1051より指定された決済機能の有無を参照して対応する部分の設定を行う。また、EMDサービスセンタ102は、リボケーションリストをチェックしてSAM登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由にEMDサービスセンタ102によって使用が禁止されている（無効な）SAMのリストである。また、EMDサービスセンタ102は、決済時にはSAM1051に対応するSAM登録リストを取り出し、その中に記述されたSAMがリボケーションリストに含まれているかを確認する。また、EMDサービスセンタ102は、SAM登録リストに署名を添付する。なお、SAMリボケーションリストは、同一系の（同一のバス191に接続されている）SAMのみを対象として生成され、各SAMに対応するリボケーションフラグによって、当該SAMの有効および無効を示している。

【0196】以下、図1に示すコンテンツプロバイダ101の全体動作について説明する。図29は、コンテンツプロバイダ101の全体動作のフローチャートである。

ステップS1：EMDサービスセンタ102は、コンテンツプロバイダ101が所定の登録処理を経た後に、コンテンツプロバイダ101の公開鍵データK_{CP,P}の公開鍵証明書CER_{CP}をコンテンツプロバイダ101に送信する。また、EMDサービスセンタ102は、SAM1051～1054が所定の登録処理を経た後に、SAM1051～1054の公開鍵データK_{SAM1,P}～K_{SAM4,P}の公開鍵証明書CER_{CP1}～CER_{CP4}をSAM1051～1054に送信する。また、EMDサービスセンタ102は、相互認証を行った後に、各々有効期限が1カ

月の6カ月分の配信用鍵データKD₁～KD₆をコンテンツプロバイダ101に送信し、3カ月分の配信用鍵データKD₁～KD₃をユーザホームネットワーク103に送信する。このように、EMDシステム100では、配信用鍵データKD₁～KD₃を予めSAM105₁～105₄に配給しているため、SAM105₁～105₄とEMDサービスセンタ102との間がオフラインの状態でも、SAM105₁～105₄においてコンテンツプロバイダ101から配給されたセキュアコンテンツ104を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ108に記述され、利用履歴データ108は、SAM105₁～105₄とEMDサービスセンタ102とが接続されたときに、EMDサービスセンタ102に自動的に送信されるため、EMDサービスセンタ102における決済処理を確実に行うことができる。なお、EMDサービスセンタ102が、所定の期間内に、利用履歴データ108を回収できないSAMについては、リボケーションリストで無効の対象とする。なお、利用制御状態データ166は、原則として、リアルタイムで、SAM105₁～105₄からEMDサービスセンタ102に送信される。

【0197】ステップS2：コンテンツプロバイダ101は、相互認証を行った後に、図6(A)に示す権利登録要求モジュールMod₂を、EMDサービスセンタ102に送信する。そして、EMDサービスセンタ102は、所定の署名検証を行った後に、権利書データ106およびコンテンツ鍵データK_cを登録して権威化する。

【0198】ステップS3：コンテンツプロバイダ101は、対応する期間の配信用鍵データKD₁～KD₆などを用いて暗号化を行って、図4(A)、(B)に示すコンテンツファイルCFおよびキーファイルKFを作成し、これらと図4(C)に示す公開鍵証明書データCER_{cp}とを格納したセキュアコンテンツ104を、オンラインおよび／またはオフラインで、ユーザホームネットワーク103に配給する。

【0199】ステップS4：ユーザホームネットワーク103のSAM105₁～SAM105₄は、セキュアコンテンツ104に対応する期間の配信用鍵データKD₁～KD₃などを用いて復号し、セキュアコンテンツ104の作成者および送信者と正当性を検証するための署名検証などを行い、セキュアコンテンツ104が正当なコンテンツプロバイダ101から送信されたか否かを確認する。

【0200】ステップS5：SAM105₁～SAM105₄において、ユーザによる図9に示す購入・利用形態決定操作部165の操作に応じた操作信号S165に基づいて、購入・利用形態を決定する。このとき、図15に示す利用監視部186において、セキュアコンテンツ104に格納された権利書データ106に基づいて、ユーザによるコンテンツファイルCFの購入・利用形態が

管理される。

【0201】ステップS6：SAM105₁～SAM105₄の図15に示す課金処理部187において、操作信号S165に基づいて、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ108および利用制御状態データ166が生成し、これらをEMDサービスセンタ102に送信する。

【0202】ステップS7：EMDサービスセンタ102は、図8に示す決算処理部142において、利用履歴データ108に基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を作成する。EMDサービスセンタ102は、決済請求権データ152およびその署名データSIG₉₉を、図1に示すペイメントゲートウェイ90を介して、決済機関91に送信する。また、EMDサービスセンタ102は、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0203】ステップS8：決済機関91において、署名データSIG₉₉の検証を行った後に、決済請求権データ152に基づいて、ユーザが支払った金額が、コンテンツプロバイダ101の所有者に分配される。

【0204】第1実施形態の第1変形例

上述した実施形態では、図4(B)に示すように、コンテンツプロバイダ101において配信用鍵データKDを用いてキーファイルKFを暗号化し、SAM105₁～105₄において配信用鍵データKDを用いてキーファイルKFを復号する場合を例示したが、図1に示すように、コンテンツプロバイダ101からSAM105₁～105₄にセキュアコンテンツ104を直接供給する場合には、配信用鍵データKDを用いたキーファイルKFの暗号化は必ずしも行なわなくてもよい。このように、配信用鍵データKDを用いてキーファイルKFを暗号化することは、後述する第2実施形態のように、コンテンツプロバイダからユーザホームネットワークにサービスプロバイダを介してコンテンツデータを供給する場合に、配信用鍵データKDをコンテンツプロバイダおよびユーザホームネットワークにのみ保持させることで、サービスプロバイダによる不正行為を抑制する際に大きな効果を発揮する。但し、上述した第1実施形態の場合でも、配信用鍵データKDを用いてキーファイルKFを暗号化することは、コンテンツデータの不正利用の抑制力を高める点で効果がある。

【0205】また、上述した実施形態では、図4(B)に示すキーファイルKF内の権利書データ106内に標準小売価格データSRPを格納する場合を例示したが、セキュアコンテンツ104内のキーファイルKFの外に、標準小売価格データSRP(プライスタグデータ)を格納してもよい。この場合には、標準小売価格データSRPに対して秘密鍵データK_{cp}を用いて作成した署名データを添付する。

10

20

30

40

50

【0206】第1実施形態の第2変形例

上述した第1実施形態では、図1に示すように、EMDサービスセンタ102が、自らが生成した決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91で決済処理を行なう場合を例示したが、例えば、図30に示すように、EMDサービスセンタ102からコンテンツプロバイダ101に決済請求権データ152を送信し、コンテンツプロバイダ101自らが、決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91に対して決済処理を行なってもよい。

【0207】第1実施形態の第3変形例

上述した第1実施形態では、単数のコンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁～105₄に、セキュアコンテナ104を供給する場合を例示したが、2以上のコンテンツプロバイダ101a, 101bからSAM105₁～105₄にそれぞれセキュアコンテナ104a, 104bを供給するようにしてもよい。図31は、コンテンツプロバイダ101a, 101bを用いる場合の第1実施形態の第2変形例に係わるEMDシステムの構成図である。この場合には、EMDサービスセンタ102は、コンテンツプロバイダ101aおよび101bに、それぞれ6か月分の配信用鍵データKD_{a1}～KD_{a6}およびKD_{b1}～KD_{b6}を配信する。また、EMDサービスセンタ102は、SAM105₁～105₄に、3か月分の配信用鍵データKD_{a1}～KD_{a3}およびKD_{b1}～KD_{b3}を配信する。

【0208】そして、コンテンツプロバイダ101aは、独自のコンテンツ鍵データKc_aを用いて暗号化したコンテンツファイルCF_aと、コンテンツ鍵データKc_aおよび権利書データ106aなどを対応する期間の配信用鍵データKD_{a1}～KD_{a6}を用いて暗号化したキーファイルKF_aとを格納したセキュアコンテナ104aをSAM105₁～105₄にオンラインおよび／またはオフランで供給する。このとき、キーファイルの識別子として、EMDサービスセンタ102が配付するグローバルユニークな識別子Content_IDが用いられ、EMDサービスセンタ102によって、コンテンツデータが一元的に管理される。また、コンテンツプロバイダ101bは、独自のコンテンツ鍵データKc_bを用いて暗号化したコンテンツファイルCF_bと、コンテンツ鍵データKc_bおよび権利書データ106bなどを対応する期間の配信用鍵データKD_{b1}～KD_{b6}を用いて暗号化したキーファイルKF_bとを格納したセキュアコンテナ104bをSAM105₁～105₄にオンラインおよび／またはオフランで供給する。

【0209】SAM105₁～105₄は、セキュアコンテナ104aについては、対応する期間の配信用鍵データKD_{a1}～KD_{a3}を用いて復号を行い、所定の署

名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108aおよび利用制御状態データ166aをEMDサービスセンタ102に送信する。また、SAM105₁～105₄は、セキュアコンテナ104bについては、対応する期間の配信用鍵データKD_{b1}～KD_{b3}を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108bおよび利用制御状態データ166bをEMDサービスセンタ102に送信する。

【0210】EMDサービスセンタ102では、利用履歴データ108aに基づいて、コンテンツプロバイダ101aについての決済請求権データ152aを作成し、これを用いて決済機関91に対して決済処理を行なう。また、EMDサービスセンタ102では、利用履歴データ108bに基づいて、コンテンツプロバイダ101bについての決済請求権データ152bを作成し、これを用いて決済機関91に対して決済処理を行なう。

【0211】また、EMDサービスセンタ102は、権利書データ106a, 106bを登録して権威化を行なう。このとき、EMDサービスセンタ102は、権利書データ106a, 106bに対応するキーファイルKF_a, KF_bに対して、グローバルユニークな識別子Content_IDを配付する。また、EMDサービスセンタ102は、コンテンツプロバイダ101a, 101bの公開鍵証明書データCER_{cpa}, CER_{cpb}を発行し、これに自らの署名データSIG_{1b}, ESC, SIG_{1a}, ESCを付してその正当性を認証する。

【0212】第2実施形態

上述した実施形態では、コンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁～105₄にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのSAMに配給する場合について説明する。

【0213】図32は、本実施形態のEMDシステム300の構成図である。図32に示すように、EMDシステム300は、コンテンツプロバイダ301、EMDサービスセンタ302、ユーザホームネットワーク303、サービスプロバイダ310、ペイメントゲートウェイ90および決済機関91を有する。コンテンツプロバイダ301、EMDサービスセンタ302、SAM305₁～305₄などおよびサービスプロバイダ310は、それぞれ請求項22などに係わるデータ提供装置、管理装置、データ処理装置およびデータ配給装置にそれぞれ対応している。コンテンツプロバイダ301は、サービスプロバイダ310に対してコンテンツデータを供給する点を除いて、前述した第1実施形態のコンテン

プロバイダ101と同じである。また、EMDサービスセンタ302は、コンテンツプロバイダ101およびSAM5051~5054に加えて、サービスプロバイダ310に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第1実施形態のEMDサービスセンタ102と同じである。また、ユーザホームネットワーク303は、ネットワーク機器3601およびAV機器3602~3604を有している。ネットワーク機器3601はSAM3051およびCAモジュール311を内蔵しており、AV機器3602~3604はそれぞれSAM3052~3054を内蔵している。ここで、SAM3051~3054は、サービスプロバイダ310からセキュアコンテナ304の配給を受ける点と、コンテンツプロバイダ301に加えてサービスプロバイダ310についての署名データの検証処理およびSP用購入履歴データ（データ配給装置用購入履歴データ）309の作成を行なう点とを除いて、前述した第1実施形態のSAM1051~1054と同じである。

【0214】先ず、EMDシステム300の概要について説明する。EMDシステム300では、コンテンツプロバイダ301は、自らが提供しようとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す前述した第1実施形態と同様の権利書(UCP:Usage Control Policy)データ106を、高い信頼性のある権威機関であるEMDサービスセンタ302に送信する。権利書データ106は、EMDサービスセンタ302に登録されて権威化（認証）される。

【0215】また、コンテンツプロバイダ301は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成する。また、コンテンツプロバイダ301は、EMDサービスセンタ302から配給された対応する期間の配信用鍵データKD1~KD6を用いて、コンテンツ鍵データKcおよび権利書データ106を暗号化し、それらを格納したキーファイルKFを作成する。そして、コンテンツプロバイダ301は、コンテンツファイルCF、キーファイルKFおよび自らの署名データとを格納したセキュアコンテナ104を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いて、あるいはオフラインなどでサービスプロバイダ310に供給する。

【0216】サービスプロバイダ310は、コンテンツプロバイダ301からセキュアコンテナ104を受け取ると、署名データの検証を行なって、セキュアコンテナ104が正当なコンテンツプロバイダ301によって作成されたものであるか、並びに送り主の正当性を確認する。次に、サービスプロバイダ310は、例えばオフラインで通知されたコンテンツプロバイダ301が希望するコンテンツに対しての価格（SRP）に、自らのサー

ビスの価格を加算した価格を示すプライスタグデータ（PT）312を作成する。そして、サービスプロバイダ310は、セキュアコンテナ104から取り出したコンテンツファイルCFおよびキーファイルKFと、プライスタグデータ312と、これらに対する自らの秘密鍵データKsp,sによる署名データとを格納したセキュアコンテナ304を作成する。このとき、キーファイルKFは、配信用鍵データKD1~KD6によって暗号化されており、サービスプロバイダ310は当該配信用鍵データKD1~KD6を保持していないため、サービスプロバイダ310はキーファイルKFの中身を見たり、書き換えたりすることはできない。また、EMDサービスセンタ302は、プライスタグデータ312を登録して権威化する。

【0217】サービスプロバイダ310は、オンラインおよび／またはオフラインでセキュアコンテナ304をユーザホームネットワーク303に配給する。このとき、オフラインの場合には、セキュアコンテナ304はSAM3051~3054にそのまま供給される。一方、オンラインの場合には、サービスプロバイダ310とCAモジュール311との間で相互認証を行い、セキュアコンテナ304をサービスプロバイダ310においてセッション鍵データKsesを用いた暗号化して送信し、CAモジュール311において受信したセキュアコンテナ304をセッション鍵データKsesを用いて復号した後に、SAM3051~3054に転送する。

【0218】次に、SAM3051~3054において、セキュアコンテナ304を、EMDサービスセンタ302から配給された対応する期間の配信用鍵データKD1~KD3を用いて復号した後に、署名データの検証処理を行う。SAM3051~3054に供給されたセキュアコンテナ304は、ネットワーク機器3601およびAV機器3602~3604において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。SAM3051~3054は、上述したセキュアコンテナ304の購入・利用の履歴を利用履歴(Usage Log)データ308として記録する。利用履歴データ（履歴データまたは管理装置用履歴データ）308は、例えば、EMDサービスセンタ302からの要求に応じて、ユーザホームネットワーク303からEMDサービスセンタ302に送信される。

【0219】EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101およびサービスプロバイダ310に分配され

る。

【0220】本実施形態では、EMDサービスセンタ302は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。すなわち、EMDサービスセンタ302は、中立の立場にある最高の権威機関であるルート認証局92に対してのセカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051～3054において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ302の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ301の権利書データ106およびサービスプロバイダ310のプライスタグデータ312を登録して権威化することも、EMDサービスセンタ302の認証機能によるものである。また、EMDサービスセンタ302は、例えば、配信用鍵データKD1～KD6などの鍵データの管理を行なう鍵データ管理機能を有する。また、EMDサービスセンタ302は、コンテンツプロバイダ301が登録した権利書データ106とSAM3051～SAM3054から入力した利用履歴データ308とサービスプロバイダ310が登録したプライスタグデータ312とに基づいて、ユーザホームネットワーク303のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ301およびサービスプロバイダ310に分配して支払う権利処理（利益分配）機能を有する。

【0221】以下、コンテンツプロバイダ301の各構成要素について詳細に説明する。

〔コンテンツプロバイダ301〕図33は、コンテンツプロバイダ301の機能ブロック図であり、サービスプロバイダ310との間で送受信されるデータに関連するデータの流れが示されている。図33に示すように、コンテンツプロバイダ301は、コンテンツマスタソースサーバ111、電子透かし情報付加部112、圧縮部113、暗号化部114、乱数発生部115、暗号化部116、署名処理部117、セキュアコンテンツ作成部118、セキュアコンテンツデータベース118a、記憶部119、相互認証部120、暗号化・復号部121、権利書データ作成部122、EMDサービスセンタ管理部125およびサービスプロバイダ管理部324を有する。

【0222】図33において、図2と同一符号を付した構成要素は、前述した第1実施形態において図2および図3を参照しながら説明した同一符号の構成要素と同じである。すなわち、コンテンツプロバイダ301は、図2に示すSAM管理部124の代わりにサービスプロバイダ管理部324を設けた構成をしている。サービスプロバイダ管理部324は、セキュアコンテンツ作成部118から入力したセキュアコンテンツ104を、オフライン

および／またはオンラインで、図32に示すサービスプロバイダ310に提供する。セキュアコンテンツ104には、第1実施形態と同様に、図4(A)、(B)、

(C)に示すコンテンツファイルCFおよびその署名データSIG6.cpと、キーファイルKFおよびその署名データSIG7.cpと、公開鍵証明書データCER.cpおよびその署名データSIG1.escとが格納されている。

【0223】サービスプロバイダ管理部324は、セキュアコンテンツ104をオンラインでサービスプロバイダ310に配信する場合には、暗号化・復号部121においてセッション鍵データKsesを用いてセキュアコンテンツ104を暗号化した後に、ネットワークを介してサービスプロバイダ310に配信する。

【0224】また、図3に示すしたコンテンツプロバイダ101内でのデータの流は、サービスプロバイダ310にも同様に適用される。

【0225】〔サービスプロバイダ310〕サービスプロバイダ310は、コンテンツプロバイダ301から提供を受けたセキュアコンテンツ104内のコンテンツファイルCFおよびキーファイルKFと、自らが生成したプライスタグデータ312とを格納したセキュアコンテンツ304を、オンラインおよび／またはオフラインで、ユーザホームネットワーク303のネットワーク機器3601およびAV機器3602～3604に配給する。サービスプロバイダ310によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、CM(広告)に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【0226】図34は、サービスプロバイダ310の機能ブロック図である。なお、図34には、コンテンツプロバイダ301から供給を受けたセキュアコンテンツ104に応じたセキュアコンテンツ304をユーザホームネットワーク303に供給する際のデータの流れが示されている。図34に示すように、サービスプロバイダ310は、コンテンツプロバイダ管理部350、記憶部351、相互認証部352、暗号化・復号部353、署名処理部354、セキュアコンテンツ作成部355、セキュアコンテンツデータベース355a、プライスタグデータ作成部356、ユーザホームネットワーク管理部357、EMDサービスセンタ管理部358およびユーザ嗜好フィルタ生成部920を有する。

【0227】以下、コンテンツプロバイダ301から供給を受けたセキュアコンテンツ104からセキュアコンテンツ304を作成し、これをユーザホームネットワーク3

03に配給する際のサービスプロバイダ310内での処理の流れを図34を参照しながら説明する。コンテンツプロバイダ管理部350は、オンラインおよび／またはオフラインで、コンテンツプロバイダ301から図4に示すセキュアコンテナ104の供給を受けてセキュアコンテナ104を記憶部351に書き込む。このとき、コンテンツプロバイダ管理部350は、オンラインの場合には、図33に示す相互認証部120と図34に示す相互認証部352との間の相互認証によって得られたセッション鍵データKSESを用いて、セキュアコンテナ104を暗号化・復号部353において復号した後に、記憶部351に書き込む。

【0228】次に、署名処理部354において、記憶部351に記憶されているセキュアコンテナ104の図4(C)に示す署名データSIG_{1,ESC}を、記憶部351から読み出したEMDサービスセンタ302の公開鍵データK_{ESC,P}を用いて検証し、その正当性が認められた後に、図4(C)に示す公開鍵証明書データCER_{CP}から公開鍵データK_{CP,P}を取り出す。次に、署名処理部354は、当該取り出した公開鍵データK_{CP,P}を用いて、記憶部351に記憶されているセキュアコンテナ104の図4(A)、(B)に示す署名データSIG_{6,CP}、SIG_{7,CP}の検証を行う。

【0229】次に、セキュアコンテナ作成部355は、署名データSIG_{6,CP}、SIG_{7,CP}の正当性が確認されると、記憶部351からコンテンツファイルCFと、キーファイルKFと、サービスプロバイダ310の公開鍵証明書データCER_{SP}およびその署名データSIG_{61,ESC}とを読み出す。

【0230】また、プライスタグデータ作成部356は、例えばコンテンツプロバイダ301からオフラインで通知されたコンテンツプロバイダ301が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ312を作成し、これをセキュアコンテナ作成部355に出力する。

【0231】また、署名処理部354は、コンテンツファイルCF、キーファイルKFおよびプライスタグデータ312のハッシュ値をとり、サービスプロバイダ310の秘密鍵データK_{SP,P}を用いて、署名データSIG_{62,SP}、SIG_{63,SP}、SIG_{64,SP}を作成し、これをセキュアコンテナ作成部355に出力する。

【0232】次に、セキュアコンテナ作成部355は、図35(A)～(D)に示すように、コンテンツファイルCFおよびその署名データSIG_{62,SP}と、キーファイルKFおよびその署名データSIG_{63,ESC}と、プライスタグデータ312およびその署名データSIG_{64,SP}と、公開鍵証明書データCER_{SP}およびその署名データSIG_{61,ESC}とを格納したセキュアコンテナ304を作成し、セキュアコンテナデータベース355aに格納する。そして、セキュアコンテナ作成部355は、ユーザ

ホームネットワーク303からの要求に応じたセキュアコンテナ304をセキュアコンテナデータベース355aから読み出してユーザホームネットワーク管理部357に出力する。このとき、セキュアコンテナ304は、複数のコンテンツファイルCFと、それらにそれぞれ対応した複数のキーファイルKFとを格納した複合コンテナであってもよい。例えば、単数のセキュアコンテナ304内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイルCFを単数のセキュアコンテナ304に格納してもよい。これらの複数のコンテンツファイルCFなどは、ディレクトリ構造でセキュアコンテナ304内に格納してもよい。

【0233】また、セキュアコンテナ304は、デジタル放送で送信される場合には、MHEG(Multimedia and Hypermedia information coding Experts Group)プロトコルが用いられ、インターネットで送信される場合にはXML/SMIL/HTML(Hyper TextMarkup Language)プロトコルが用いられる。このとき、コンテンツファイルCFおよびキーファイルKFは、コンテンツプロバイダ301によって一元的に管理され、セキュアコンテナ304を送信するプロトコルに依存しない。すなわち、コンテンツファイルCFおよびキーファイルKFは、MHEGおよびHTMLのプロトコルをトンネリングした形でセキュアコンテナ304内に格納される。

【0234】次に、ユーザホームネットワーク管理部357は、セキュアコンテナ304を、オフラインおよび／またはオンラインでユーザホームネットワーク303に供給する。ユーザホームネットワーク管理部357は、セキュアコンテナ304をオンラインでユーザホームネットワーク303のネットワーク機器360₁に配信する場合には、相互認証後に、暗号化・復号部352においてセッション鍵データKSESを用いてセキュアコンテナ304を暗号化した後に、ネットワークを介してネットワーク機器360₁に配信する。

【0235】なお、ユーザホームネットワーク管理部357は、セキュアコンテナ304を例えば衛星などを介して放送する場合には、セキュアコンテナ304をスクランブル鍵データK_{SCR}を用いて暗号化する。また、スクランブル鍵データK_{SCR}をワーク鍵データK_Wを暗号化し、ワーク鍵データK_Wをマスタ鍵データK_Mを用いて暗号化する。そして、ユーザホームネットワーク管理部357は、セキュアコンテナ304と共に、スクランブル鍵データK_{SCR}およびワーク鍵データK_Wを、衛星を介してユーザホームネットワーク303に送信する。また、例えば、マスタ鍵データK_Mを、ICカードなどに記憶してオフラインでユーザホームネットワーク303に配給する。

【0236】また、ユーザホームネットワーク管理部357は、ユーザホームネットワーク303から、当該サ

ービスプロバイダ310が配給したコンテンツデータC
 に関してのSP用購入履歴データ309を受信すると、
 これを記憶部351に書き込む。サービスプロバイダ3
 10は、将来のサービス内容を決定する際に、SP用購
 入履歴データ309を参照する。また、ユーザ嗜好フ
 イルタ生成部920は、SP用購入履歴データ309に基
 づいて、当該SP用購入履歴データ309を送信したS
 AM3051~3054のユーザの嗜好を分析してユー
 ザ嗜好フィルタデータ900を生成し、これをユーザホ
 ームネットワーク管理部357を介してユーザホームネ
 ットワーク303のCAモジュール311に送信する。

【0237】図36には、サービスプロバイダ310内
 におけるEMDサービスセンタ302との間の通信に関
 連するデータの流れが示されている。なお、以下に示す
 処理を行う前提として、サービスプロバイダ310の関
 係者は、例えば、自らの身分証明書および決済処理を行
 う銀行口座などを用いて、オフラインで、EMDサービ
 スセンタ302に登録処理を行い、グローバルユニーク
 な識別子SP_IDを得ている。識別子SP_IDは、
 記憶部351に記憶される。

【0238】まず、サービスプロバイダ310が、EM
 Dサービスセンタ302に、自らの秘密鍵データK_{SP,S}
 に対応する公開鍵データK_{SP,S}の正当性を証明する公開
 鍵証明書データCER_{SP}を要求する場合の処理を図36
 を参照しながら説明する。まず、サービスプロバイダ3
 10は、真性乱数発生器を用いて乱数を発生して秘密鍵
 データK_{SP,S}を生成し、当該秘密鍵データK_{SP,S}に対応
 する公開鍵データK_{SP,P}を作成して記憶部351に記憶
 する。EMDサービスセンタ管理部358、サービスプ
 ロバイダ310の識別子SP_IDおよび公開鍵データ
 K_{SP,P}を記憶部351から読み出す。そして、EMDサ
 ービスセンタ管理部358は、識別子SP_IDおよび
 公開鍵データK_{SP,P}を、EMDサービスセンタ302に
 送信する。そして、EMDサービスセンタ管理部348
 は、当該登録に応じて、公開鍵証明書データCER_{SP}お
 よびその署名データSIG_{61,ESC}をEMDサービスセン
 タ302から入力して記憶部351に書き込む。

【0239】次に、サービスプロバイダ310が、EM
 Dサービスセンタ302にプライスタグデータ312を
 登録して権威化する場合の処理を図36を参照して説明
 する。

【0240】この場合には、署名処理部354におい
 て、プライスタグデータ作成部356が作成したプライ
 スタグデータ312と記憶部351から読み出したグロ
 ーバルユニークな識別子Content_IDとを格納
 したモジュールMod₁₀₃のハッシュ値が求められ、秘
 密鍵データK_{SP,S}を用いて署名データSIG_{80,SP}が生
 成される。また、記憶部351から公開鍵証明書データ
 CER_{SP}およびその署名データSIG_{61,ESC}が読み出さ
 れる。そして、図37に示すプライスタグ登録要求用モ

ジュールMod₁₀₂を、相互認証部352とEMDサー
 ビスセンタ302との間の相互認証によって得られたセ
 ッション鍵データK_{SES}を用いて暗号化・復号部353
 において暗号化した後に、EMDサービスセンタ管理部
 358からEMDサービスセンタ302に送信する。な
 お、モジュールMod₁₀₃に、サービスプロバイダ31
 0のグローバルユニークな識別子SP_IDを格納して
 もよい。

【0241】また、EMDサービスセンタ管理部358
 は、EMDサービスセンタ302から受信した決済レポ
 ートデータ307sを記憶部351に書き込む。

【0242】また、EMDサービスセンタ管理部358
 は、EMDサービスセンタ302から受信したマーケテ
 イング情報データ904を記憶部351に記憶する。マ
 ーケティング情報データ904は、サービスプロバイダ
 310が今後配給するコンテンツデータCを決定する際
 に参考にされる。

【0243】〔EMDサービスセンタ302〕EMDサ
 ービスセンタ302は、前述したように、認証局(C
 A:CertificateAuthority)、鍵管理(Key Management)
 局および権利処理(Rights Clearing)局としての役割を
 果たす。図38は、EMDサービスセンタ302の機能
 の構成図である。図38に示すように、EMDサービス
 センタ302は、鍵サーバ141、鍵データベース14
 1a、決済処理部442、署名処理部443、決算機関
 管理部144、証明書・権利書管理部445、CERデ
 ータベース445a、コンテンツプロバイダ管理部14
 8、CPデータベース148a、SAM管理部149、
 SAMデータベース149a、相互認証部150、暗号
 化・復号部151、サービスプロバイダ管理部390、
 SPデータベース390a、ユーザ嗜好フィルタ生成部
 901およびマーケティング情報データ生成部902を
 有する。図38において、図7および図8と同じ符号を
 付した機能ブロックは、第1実施形態で説明した同一符
 号の機能ブロックと略同じ機能を有している。以下、図
 38において、新たな符号を付した機能ブロックについ
 て説明する。なお、図38には、EMDサービスセンタ
 302内の機能ブロック相互間のデータの流れのうち、
 サービスプロバイダ310との間で送受信されるデータ
 に関連するデータの流れが示されている。また、図39
 には、EMDサービスセンタ302内の機能ブロック相
 互間のデータの流れのうち、コンテンツプロバイダ30
 1との間で送受信されるデータに関連するデータの流れ
 が示されている。また、図40には、EMDサービスセ
 ンタ302内の機能ブロック相互間のデータの流れのう
 ち、図32に示すSAM3051~3054および決済
 機関91との間で送受信されるデータに関連するデータ
 の流れが示されている。

【0244】決済処理部442は、図40に示すよう
 に、SAM3051~3054から入力した利用履歴デ

ータ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびプライスタグデータ312に基づいて決済処理を行う。なお、この際に、決済処理部442は、サービスプロバイダ310によるダンプの有無などを監視する。決済処理部442は、決済処理により、図40に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ152cを作成し、これらをそれぞれコンテンツプロバイダ管理部148および決算機関管理部144に出力する。また、決済処理により、図38および図40に示すように、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sを作成し、これらをそれぞれサービスプロバイダ管理部390および決算機関管理部144に出力する。ここで、決済請求権データ152c、152sは、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータである。

【0245】ここで、利用履歴データ308は、第1実施形態で説明した利用履歴データ108と同様に、セキュアコンテナ304に関連したライセンス料の支払いを決定する際に用いられる。利用履歴データ308には、例えば、図41に示すように、セキュアコンテナ304に格納されたコンテンツデータCの識別子Content_ID、セキュアコンテナ304に格納されたコンテンツデータCを提供したコンテンツプロバイダ301の識別子CP_ID、セキュアコンテナ304を配給したサービスプロバイダ310の識別子SP_ID、コンテンツデータCの信号諸元データ、セキュアコンテナ304内のコンテンツデータCの圧縮方法、セキュアコンテナ304を記録した記録媒体の識別子Media_ID、セキュアコンテナ304を配給を受けたSAM3051~3054の識別子SAM_ID、当該SAM1051~1054のユーザのUSER_IDなどが記述されている。従って、EMDサービスセンタ302は、コンテンツプロバイダ301およびサービスプロバイダ310の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク303のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータおよび決済請求権データを作成する。

【0246】証明書・権利書管理部445は、CERデータベース445aに登録されて権威化された公開鍵証明書データCERcp、公開鍵証明書データCERspおよび公開鍵証明書データCERsam1~CERsam2などを読み出すと共に、コンテンツプロバイダ301の権利書データ106およびコンテンツ鍵データKc、並びにサービスプロバイダ310のプライスタグデータ312などをCERデータベース445aに登録して権威化する。このとき、証明書・権利書管理部445は、権利書デー

タ106、コンテンツ鍵データKcおよびプライスタグデータ312などのハッシュ値を取り、秘密鍵データKESC,sを用いた署名データを付して権威化証明書データを作成する。

【0247】コンテンツプロバイダ管理部148は、コンテンツプロバイダ101との間で通信する機能を有し、登録されているコンテンツプロバイダ101の識別子CP_IDなどを管理するCPデータベース148aにアクセスできる。

10 【0248】ユーザ嗜好フィルタ生成部901は、利用履歴データ308に基づいて、当該利用履歴データ308を送信したSAM3051~3054のユーザの嗜好に応じたコンテンツデータCを選択するためのユーザ嗜好フィルタデータ903を生成し、ユーザ嗜好フィルタデータ903をSAM管理部149を介して、当該利用履歴データ308を送信したSAM3051~3054に送信する。

20 【0249】マーケティング情報データ生成部902は、利用履歴データ308に基づいて、例えば、複数のサービスプロバイダ310によってユーザホームネットワーク103に配給されたコンテンツデータCの全体の購入状況などを示すマーケティング情報データ904を生成し、これをサービスプロバイダ管理部390を介して、サービスプロバイダ310に送信する。サービスプロバイダ310は、マーケティング情報データ904を参考にして、今後提供するサービスの内容を決定する。

30 【0250】以下、EMDサービスセンタ302内での処理の流れを説明する。EMDサービスセンタ302からコンテンツプロバイダ301への配信用鍵データKD1~KD6の送信と、EMDサービスセンタ302からSAM3051~3054への配信用鍵データKD1~KD3の送信とは、第1実施形態の場合と同様に行なわれる。

【0251】また、EMDサービスセンタ302がコンテンツプロバイダ301から、公開鍵証明書データの発行要求を受けた場合の処理も、証明書・権利書管理部445がCERデータベース445aに対して登録を行なう点を除いて、前述した第1実施形態の場合と同様に行なわれる。

40 【0252】次に、EMDサービスセンタ302がサービスプロバイダ310から、公開鍵証明書データの発行要求を受けた場合の処理を、図38を参照しながら説明する。この場合に、サービスプロバイダ管理部390は、予めEMDサービスセンタ302によって与えられたサービスプロバイダ310の識別子SP_ID、公開鍵データKsp,pおよび署名データSIG70,spをサービスプロバイダ310から受信すると、これらを、相互認証部150と図34に示す相互認証部352と間の相互認証で得られたセッション鍵データKsesを用いて復号する。そして、当該復号した署名データSIG70,spの

正当性を署名処理部443において確認した後に、識別子SP_IDおよび公開鍵データK_{SP,P}に基づいて、当該公開鍵証明書データの発行要求を出したサービスプロバイダ310がSPデータベース390aに登録されているか否かを確認する。そして、証明書・権利書管理部445は、当該サービスプロバイダ310の公開鍵証明書データCER_{SP}をCERデータベース445aから読み出してサービスプロバイダ管理部390に出力する。た、署名処理部443は、公開鍵証明書データCER_{SP}のハッシュ値をとり、EMDサービスセンタ302の秘密鍵データK_{ESC,S}を用いて、署名データSIG_{61,ESC}を作成し、これをサービスプロバイダ管理部390に出力する。そして、サービスプロバイダ管理部390は、公開鍵証明書データCER_{SP}およびその署名データSIG_{61,ESC}を、相互認証部150と図34に示す相互認証部352と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、サービスプロバイダ310に送信する。

【0253】なお、EMDサービスセンタ302がSAM1051~1054から、公開鍵証明書データの発行要求を受けた場合の処理は、第1実施形態と同様である。また、EMDサービスセンタ302が、コンテンツプロバイダ301から権利書データ106の登録要求を受けた場合の処理も、第1実施形態と同様である。

【0254】次に、EMDサービスセンタ302が、サービスプロバイダ310からプライスタグデータ312の登録要求を受けた場合の処理を、図38を参照しながら説明する。この場合には、サービスプロバイダ管理部390がサービスプロバイダ310から図37に示すプライスタグ登録要求モジュールMod₁₀₂を受信すると、相互認証部150と図34に示す相互認証部352と間の相互認証で得られたセッション鍵データK_{SES}を用いてプライスタグ登録要求モジュールMod₁₀₂を復号する。そして、当該復号したプライスタグ登録要求モジュールMod₁₀₂に格納された署名データSIG_{80,SP}の正当性を署名処理部443において確認した後に、プライスタグ登録要求モジュールMod₁₀₂に格納されたプライスタグデータ312を、証明書・権利書管理部445を介してCERデータベース445aに登録して権威化する。

【0255】次に、EMDサービスセンタ302において決済を行なう場合の処理を図40を参照しながら説明する。SAM管理部149は、ユーザホームネットワーク303の例えばSAM3051から利用履歴データ308およびその署名データSIG_{205,SAM1}を入力すると、利用履歴データ308および署名データSIG_{205,SAM1}を、相互認証部150とSAM3051~3054との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号し、SAM3051の公開鍵データK_{SAM1,P}を用いて署名データSIG_{205,SAM1}の検証

を行なった後に、決算処理部442に出力する。

【0256】そして、決済処理部442は、SAM3051から入力した利用履歴データ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびプライスタグデータ312とに基づいて決済処理を行う。決済処理部442は、決済処理により、図40に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ152cを作成し、これらをそれぞれコンテンツプロバイダ管理部148および決算機関管理部144に出力する。また、決済処理により、図38および図40に示すように、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sを作成し、これらをそれぞれサービスプロバイダ管理部390および決算機関管理部144に出力する。

【0257】次に、決算機関管理部144は、決済請求権データ152c、152sと、それらについて秘密鍵データK_{ESC,S}を用いて作成した署名データとを、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図32に示すペイメントゲートウェイ90を介して決済機関91に送信する。これにより、決済請求権データ152cに示される金額の金銭がコンテンツプロバイダ301に支払われ、決済請求権データ152sに示される金額の金銭がサービスプロバイダ310に支払われる。

【0258】次に、EMDサービスセンタ302がコンテンツプロバイダ301およびサービスプロバイダ310に決済レポートデータ307cおよび307sを送信する場合の処理を説明する。決算処理部442において決済が行なわれると、決算処理部442からコンテンツプロバイダ管理部148に決済レポートデータ307cが出力される。コンテンツプロバイダ管理部148は、決算処理部442から決済レポートデータ307cを入力すると、これを、相互認証部150と図33に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ301に送信する。また、決算処理部442において決済が行なわれると、決算処理部442からサービスプロバイダ管理部390に決済レポートデータ307sが出力される。サービスプロバイダ管理部390は、決算処理部442から決済レポートデータ307sを入力すると、これを、相互認証部150と図34に示す相互認証部352と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、サービスプロバイダ310に送信する。

【0259】EMDサービスセンタ302は、その他に、第1実施形態のEMDサービスセンタ102と同様に、SAM3051~3054の出荷時の処理と、SAM登録リストの登録処理とを行なう。

【0260】〔ユーザホームネットワーク303〕ユー

ザホームネットワーク 303 は、図 32 に示すように、ネットワーク機器 3601 および A/V 機器 3602 ~ 3604 を有している。ネットワーク機器 3601 は、CA モジュール 311 および SAM 3051 を内蔵している。また、A/V 機器 3602 ~ 3604 は、それぞれ SAM 3052 ~ 3054 を内蔵している。SAM 3051 ~ 3054 の相互間は、例えば、1394 シリアルインタフェースバスなどのバス 191 を介して接続されている。なお、A/V 機器 3602 ~ 3604 は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス 191 を介してネットワーク機器 3601 のネットワーク通信機能を利用してもよい。また、ユーザホームネットワーク 303 は、ネットワーク機能を有していない A/V 機器のみを有していてもよい。

【0261】以下、ネットワーク機器 3601 について説明する。図 42 は、ネットワーク機器 3601 の構成図である。図 42 に示すように、ネットワーク機器 3601 は、通信モジュール 162、CA モジュール 311、復号モジュール 905、SAM 3051、復号・伸
20 長モジュール 163、購入・利用形態決定操作部 165、ダウンロードメモリ 167、再生モジュール 169 および外部メモリ 201 を有する。図 42 において、図 8 と同一符号を付した構成要素は、第 1 実施形態で説明した同一符号の構成要素と同じである。

【0262】通信モジュール 162 は、サービスプロバイダ 310 との間の通信処理を行なう。具体的には、通信モジュール 162 は、サービスプロバイダ 310 から衛星放送などで受信したセキュアコンテンツ 304 を復号モジュール 905 に出力する。また、通信モジュール 1
30 62 は、サービスプロバイダ 310 に電話回線などを介して SP 用購入履歴データ 309 を受信したユーザ嗜好フィルタデータ 900 を CA モジュール 311 に出力すると共に、CA モジュール 311 から入力した SP 用購入履歴データ 309 を電話回線などを介してサービスプロバイダ 310 に送信する。

【0263】図 43 は、CA モジュール 311 および復号モジュール 905 の機能ブロック図である。図 43 に示すように、CA モジュール 311 は、相互認証部 906、記憶部 907、暗号化・復号部 908 および SP 用
40 購入履歴データ生成部 909 を有する。相互認証部 906 は、CA モジュール 311 とサービスプロバイダ 310 との間で電話回線を介してデータを送受信する際に、サービスプロバイダ 310 との間で相互認証を行ってセッション鍵データ KSES を生成し、これを暗号化・復号部 908 に出力する。

【0264】記憶部 907 は、例えば、サービスプロバイダ 310 とユーザとの間で契約が成立した後に、サービスプロバイダ 310 から IC カード 912 などを用いてオフラインで供給されたマスタ鍵データ KM を記憶す
50

る。

【0265】暗号化・復号部 908 は、復号モジュール 905 の復号部 910 からそれぞれ暗号化されたスクランブル鍵データ KSCR およびワーク鍵データ KW を入力し、記憶部 907 から読み出したマスタ鍵データ KM を用いてワーク鍵データ KW を復号する。そして、暗号化・復号部 908 は、当該復号したワーク鍵データ KW を用いてスクランブル鍵データ KSCR を復号し、当該復号したスクランブル鍵データ KSCR を復号部 910 に出力する。また、暗号化・復号部 908 は、電話回線などを介して通信モジュール 162 がサービスプロバイダ 310 から受信したユーザ嗜好フィルタデータ 900 を、相互認証部 906 からのセッション鍵データ KSES を用いて復号して復号モジュール 905 のセキュアコンテンツ選択部 911 に出力する。また、暗号化・復号部 908
50 は、SP 用購入履歴データ生成部 909 から入力した SP 用購入履歴データ 309 を、相互認証部 906 からのセッション鍵データ KSES を用いて復号して通信モジュール 162 を介してサービスプロバイダ 310 に送信する。

【0266】SP 用購入履歴データ生成部 909 は、図 42 に示す購入・利用形態決定操作部 165 を用いてユーザによるコンテンツデータ C の購入操作に応じた操作信号 S165、または SAM 3051 からの利用制御状態データ 166 に基づいて、サービスプロバイダ 310 に固有のコンテンツデータ C の購入履歴を示す SP 用購入履歴データ 309 を生成し、これを暗号化・復号部 908 に出力する。SP 用購入履歴データ 309 は、例えば、サービスプロバイダ 310 が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

【0267】なお、CA モジュール 311 は、サービスプロバイダ 310 が課金機能を有している場合には、サービスプロバイダ 310 の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、CA モジュール 311 は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ 310 に送信する。

【0268】復号モジュール 905 は、復号部 910 およびセキュアコンテンツ選択部 911 を有する。復号部 910 は、通信モジュール 162 から、それぞれ暗号化されたセキュアコンテンツ 304、スクランブル鍵データ KSCR およびワーク鍵データ KW を入力する。そして、復号部 910 は、暗号化されたスクランブル鍵データ KSCR およびワーク鍵データ KW を CA モジュール 311 の暗号化・復号部 908 に出力し、暗号化・復号部 908 から復号されたスクランブル鍵データ KSCR を入力する。そして、復号部 910 は、暗号化されたセキュアコンテンツ 304 を、スクランブル鍵データ KSCR を用いて
50

復号した後に、セキュアコンテナ選択部911に出力する。

【0269】なお、セキュアコンテナ304が、MPEG2 Transport Stream方式でサービスプロバイダ310から送信される場合には、例えば、復号部910は、TS Packet内のECM(Entitlement Control Message)からスクランブル鍵データK_{SCR}を取り出し、EMM(Entitlement Management Message)からワーク鍵データK_wを取り出す。ECMには、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、EMMは、その他に、ユーザ(視聴者)毎に異なる個別試験契約情報などが含まれている。

【0270】セキュアコンテナ選択部911は、復号部910から入力したセキュアコンテナ304を、CAMジュール311から入力したユーザ嗜好フィルタデータ900を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ304を選択してSAM305₁に出力する。

【0271】次に、SAM305₁について説明する。なお、SAM305₁は、サービスプロバイダ310についての署名検証処理を行なうなど、コンテンツプロバイダ301に加えてサービスプロバイダ310についての処理を行う点を除いて、図10～図24を用いて前述した第1実施形態のSAM105₁と基本的に同様の機能および構造を有している。また、SAM305₂～305₄は、SAM305₁と基本的に同じ機能を有している。すなわち、SAM305₁～305₄は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ302との間で通信を行う。

【0272】以下、SAM305₁の機能について詳細に説明する。図44は、SAM305₁の機能の構成図である。なお、図44には、サービスプロバイダ310からセキュアコンテナ304を入力し、セキュアコンテナ304内のキーファイルKFを復号する処理に関連するデータの流れが示されている。図44に示すように、SAM305₁は、相互認証部170、暗号化・復号部171、172、173、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、署名処理部189、SAM管理部190、記憶部192、メディアSAM管理部197、スタックメモリ200、サービスプロバイダ管理部580、課金処理部587、署名処理部598および外部メモリ管理部811を有する。なお、図44に示すSAM305₁の所定の機能は、SAM105₁の場合と同様に、CPUにおいて秘密プログラムを実行することによって実現される。図44において、図10と同じ符号を付した機能ブロックは、第1実施形態で説明した同一符号の機能ブロックと同じである。

【0273】また、図42に示す外部メモリ201には、第1実施形態で説明した処理および後述する処理を経て、利用履歴データ308およびSAM登録リストが記憶される。また、スタックメモリ200には、図45に示すように、コンテンツ鍵データK_c、権利書データ(UCP)106、記憶部192のロック鍵データK_{LOC}、コンテンツプロバイダ301の公開鍵証明書データCER_{CP}、サービスプロバイダ310の公開鍵証明書データCER_{SP}、利用制御状態データ(UCS)366、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃およびプライスタグデータ312などが記憶される。

【0274】以下、SAM305₁の機能ブロックのうち、図44において新たに符号を付した機能ブロックについて説明する。署名処理部589は、記憶部192あるいはスタックメモリ200から読み出したEMDサービスセンタ302の公開鍵データK_{ESC,P}、コンテンツプロバイダ301の公開鍵データK_{CP,P}およびサービスプロバイダ310の公開鍵データK_{SP,P}を用いて、セキュアコンテナ304内の署名データの検証を行なう。

【0275】課金処理部587は、図46に示すように、図42に示す購入・利用形態決定操作部165からの操作信号S165と、スタックメモリ200から読み出されたプライスタグデータ312とに基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。課金処理部587による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御状態データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【0276】また、課金処理部587は、課金処理において、利用履歴データ308を生成し、これを外部メモリ管理部811を介して外部メモリ201に書き込む。ここで、利用履歴データ308は、第1実施形態の利用履歴データ108と同様に、EMDサービスセンタ302において、セキュアコンテナ304に関連したライセンス料の支払いを決定する際に用いられる。

【0277】また、課金処理部587は、操作信号S165に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態(UCS: Usage Control Status)データ166を生成し、これを外部メモリ管理部811を介して外部メモリ201に書き込む。コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。ここで、利用制御状態データ166は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられ

る。利用制御状態データ166には、コンテンツのID、購入形態、買い切り価格、当該コンテンツの購入が行なわれたSAMのSAM_ID、購入を行なったユーザのUSER_IDなどが記述されている。

【0278】なお、決定された購入形態が再生課金である場合には、例えば、SAM3051からサービスプロバイダ310に利用制御状態データ166をリアルタイムに送信し、サービスプロバイダ310がEMDサービスセンタ302に、利用履歴データ108をSAM1051に取りに行くことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ166が、サービスプロバイダ310およびEMDサービスセンタ302にリアルタイムに送信される。

【0279】また、SAM3051では、EMDサービスセンタ管理部185がEMDサービスセンタ302から受信したユーザ嗜好フィルタデータ903が、サービスプロバイダ管理部580に出力される。そして、サービスプロバイダ管理部580において、図42に示す復号モジュール905から入力したセキュアコンテナ304が、ユーザ嗜好フィルタデータ903に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ304が選択され、当該選択されたセキュアコンテナ304が誤り訂正部181に出力される。これにより、SAM3051において、当該SAM3051のユーザが契約している全てのサービスプロバイダ310を対象として、当該ユーザによるコンテンツデータCの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータCの選択処理が可能になる。

【0280】以下、SAM3051内での処理の流れを説明する。EMDサービスセンタ302から受信した配信用鍵データKD1~KD3を記憶部192に格納する際のSAM3051内での処理の流れは、前述したSAM1051の場合と同様である。

【0281】次に、セキュアコンテナ304をサービスプロバイダ310から入力し、セキュアコンテナ304内のキーファイルKFを復号する際のSAM3051内での処理の流れを図44を参照しながら説明する。相互認証部170と図34に示すサービスプロバイダ310の相互認証部352との間で相互認証が行なわれる。暗号化・復号部171は、当該相互認証によって得られたセッション鍵データKSESを用いて、サービスプロバイダ管理部580を介してサービスプロバイダ310から受信した図35に示すセキュアコンテナ304を復号する。

【0282】次に、署名処理部589は、図35(D)に示す署名データSIG61,ESCの検証を行なった後に、図35(D)に示す公開鍵証明書データCERSP内に格納されたサービスプロバイダ310の公開鍵データKSP,Pを用いて、署名データSIG62,SP, SI

G63,SP, SIG64,SPの正当性を確認する。サービスプロバイダ管理部580は、署名データSIG62,SP, SIG63,SP, SIG64,SPの正当性が確認されると、セキュアコンテナ304を誤り訂正部181に出力する。

【0283】誤り訂正部181は、セキュアコンテナ304を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。ダウンロードメモリ管理部182は、相互認証部170と図42に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304をダウンロードメモリ167に書き込む。

【0284】次に、ダウンロードメモリ管理部182は、相互認証部170と図42に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304に格納された図35(B)に示すキーファイルKFを読み出してセキュアコンテナ復号部183に出力する。

【0285】そして、セキュアコンテナ復号部183は、記憶部192から入力した対応する期間の配信用鍵データKD1~KD3を用いて、キーファイルKFを復号し、図35(B)に示す署名・証明書モジュールMod1に格納された署名データSIG1,ESC, SIG2,cp~SIG4,cpを署名処理部589に出力する。署名処理部589は、図35(B)に示す署名データSIG1,ESCの検証を行なった後に、公開鍵証明書データCERcp内に格納された公開鍵データKcp,Pを用いて署名データSIG2,cp~SIG4,cpの検証を行なう。

【0286】次に、セキュアコンテナ復号部183は、署名データSIG2,cp~SIG4,cpの正当性が確認されると、キーファイルKFをスタックメモリ200に書き込む。

【0287】以下、サービスプロバイダ310からダウンロードメモリ167にダウンロードされたセキュアコンテナ304の購入形態を決定するまでの処理の流れを図46を参照しながら説明する。ユーザによる図42に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が課金処理部587に出力されると、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図42に示す復号・伸長モジュール163に出力される。このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データKSESによる暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データKSESによる暗号化・復号とが行なわれる。コンテンツファイルCFは、図42に示す復号部221において復号された後に、復号部222に出力される。

【0288】また、スタックメモリ200から読み出されたコンテンツ鍵データKcおよび半開示パラメータデ

ータ 199 が、図 42 に示す復号・伸長モジュール 163 に出力される。このとき、相互認証部 170 と相互認証部 220 との間の相互認証後に、コンテンツ鍵データ Kc および半開示パラメータデータ 199 に対してセッション鍵データ Kses による暗号化および復号が行なわれる。次に、復号された半開示パラメータデータ 199 が半開示処理部 225 に出力され、半開示処理部 225 からの制御によって、復号部 222 によるコンテンツ鍵データ Kc を用いたコンテンツデータ C の復号が半開示で行われる。次に、半開示で復号されたコンテンツデータ C が、伸長部 223 において伸長された後に、電子透かし情報処理部 224 に出力される。次に、電子透かし情報処理部 224 においてユーザ電子透かし情報用データ 196 がコンテンツデータ C に埋め込まれた後、コンテンツデータ C が再生モジュール 169 において再生され、コンテンツデータ C に応じた音響が出力される。

【0289】そして、コンテンツを試聴したユーザが、購入・利用形態決定操作部 165 を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号 S165 が課金処理部 187 に出力される。そして、課金処理部 187 において、決定された購入形態に応じた利用履歴データ 308 および利用制御状態データ 166 が生成され、利用履歴データ 308 が外部メモリ管理部 811 を介して外部メモリ 201 に書き込まれると共に利用制御状態データ 166 がスタックメモリ 200 に書き込まれる。以後は、利用監視部 186 において、利用制御状態データ 166 によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。そして、スタックメモリ 200 に格納されているキーファイル KF に、利用制御状態データ 166 が加えられ、購入形態が決定した後述する図 47 に示す新たなキーファイル KF11 が生成される。キーファイル KF11 は、スタックメモリ 200 に記憶される。図 47 に示すように、キーファイル KF1 に格納された利用制御状態データ 166 はストレージ鍵データ Kstr を用いて DES の CBC モードを利用して暗号化されている。また、当該ストレージ鍵データ Kstr を MAC 鍵データとして用いて生成した MAC 値である MAC300 が付されている。また、利用制御状態データ 166 および MAC300 からなるモジュールは、メディア鍵データ Kmed を用いて DES の CBC モードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データ Kmed を MAC 鍵データとして用いて生成した MAC 値である MAC301 が付されている。

【0290】次に、ダウンロードメモリ 167 に記憶されている購入形態が既に決定されたコンテンツデータ C を再生する場合の処理の流れを、図 46 を参照しながら説明する。この場合には、利用監視部 186 の監視下で、操作信号 S165 に基づいて、ダウンロードメモリ 167 に記憶されているコンテンツファイル CF が、図

42 に示す復号・伸長モジュール 163 に出力される。また、スタックメモリ 200 から読み出されたコンテンツ鍵データ Kc が復号・伸長モジュール 163 に出力される。そして、復号・伸長モジュール 163 の復号部 222 において、コンテンツ鍵データ Kc を用いたコンテンツファイル CF の復号と、伸長部 223 による伸長処理とが行なわれ、再生モジュール 169 において、コンテンツデータ C が再生される。このとき、課金処理部 587 において、操作信号 S165 に応じて、利用履歴データ 308 が更新される。利用履歴データ 308 は、秘密鍵データ Ksam1s を用いて作成したそれぞれ署名データ SIG205、SAM1 と共に、EMD サービスセンタ管理部 185 を介して、所定のタイミングで、EMD サービスセンタ 302 に送信される。

【0291】次に、図 48 に示すように、例えば、ネットワーク機器 3601 のダウンロードメモリ 167 にダウンロードされた既に購入形態が決定されたコンテンツファイル CF を、バス 191 を介して、AV 機器 3602 の SAM3052 に転送する場合の SAM3051 内での処理の流れを図 49 を参照しながら説明する。ユーザは、購入・利用形態決定操作部 165 を操作して、ダウンロードメモリ 167 に記憶された所定のコンテンツを AV 機器 3602 に転送することを指示し、当該操作に応じた操作信号 S165 が、課金処理部 587 に出力される。これにより、課金処理部 587 は、操作信号 S165 に基づいて、スタックメモリ 200 に記憶されている利用履歴データ 308 を更新する。

【0292】また、ダウンロードメモリ管理部 182 は、ダウンロードメモリ 167 から読み出した図 50 (A) に示すコンテンツファイル CF を SAM 管理部 190 に出力する。また、スタックメモリ 200 から読み出した図 50 (B) に示す既に購入形態が決定されたキーファイル KF11 を、署名処理部 589 および SAM 管理部 190 に出力する。署名処理部 589 は、キーファイル KF11 の署名データ SIG80、SAM1 を作成し、これを SAM 管理部 190 に出力する。また、SAM 管理部 190 は、記憶部 192 から、図 50 (C) に示す公開鍵証明書データ CERsam1 およびその署名データ SIG22、ESC を読み出す。

【0293】また、相互認証部 170 は、SAM3052 との間で相互認証を行って得たセッション鍵データ Kses を暗号化・復号部 171 に出力する。SAM 管理部 190 は、図 50 (A)、(B)、(C) に示すデータを、暗号化・復号部 171 において、セッション鍵データ Kses を用いて暗号化した後に、図 49 に示す AV 機器 3602 の SAM3052 に出力する。

【0294】以下、図 48 に示すように、SAM3051 から入力したコンテンツファイル CF などを、RAM 型などの記録媒体（メディア）に書き込む際の SAM3052 内での処理の流れを、図 51 を参照しながら説明

101

する。

【0295】この場合には、SAM3052のSAM管理部190は、図51に示すように、図50(A)に示すコンテンツファイルCF、図50(B)に示すキーファイルKF11およびその署名データSIG80、SAM1と、図50(C)に示す公開鍵署名データCERSAM1およびその署名データSIG22、ESCとを、ネットワーク機器3601のSAM3051から入力する。そして、暗号化・復号部171において、SAM管理部190が入力したコンテンツファイルCFと、キーファイルKF11およびその署名データSIG80、SAM1と、公開鍵署名データCERSAM1およびその署名データSIG22、ESCとが、相互認証部170とSAM3051の相互認証部170との間の相互認証によって得られたセッション鍵データKSESを用いて復号される。

【0296】次に、セッション鍵データKSESを用いて復号されたコンテンツファイルCFがメディアSAM管理部197に出力される。また、セッション鍵データKSESを用いて復号されたキーファイルKF11およびその署名データSIG80、SAM1と、公開鍵署名データCERSAM1およびその署名データSIG22、ESCとが、スタックメモリ200に書き込まれる。

【0297】次に、署名処理部589は、スタックメモリ200から読み出した署名データSIG22、ESCを、記憶部192から読み出した公開鍵データKESC、Pを用いて検証して、公開鍵証明書データCERSAM1の正当性を確認する。そして、署名処理部589は、公開鍵証明書データCERSAM1の正当性を確認すると、公開鍵証明書データCERSAM1に格納された公開鍵データKSAM1、Pを用いて、署名データSIG80、SAM1の正当を確認する。

【0298】次に、署名データSIG80、SAM1の正当を確認されると、図50(B)に示すキーファイルKF11をスタックメモリ200から読み出して暗号化・復号部173に出力する。そして、暗号化・復号部173は、記憶部192から読み出した記録用鍵データKSTR、メディア鍵データKMEDおよび購入者鍵データKPINを用いてキーファイルKF11を順に暗号化してメディアSAM管理部197に出力する。

【0299】メディアSAM管理部197は、SAM管理部190から入力したコンテンツファイルCFおよび暗号化・復号部173から入力したキーファイルKF11を、図48に示す記録モジュール260に出力する。そして、記録モジュール260は、メディアSAM管理部197から入力したコンテンツファイルCFおよびキーファイルKF11を、図48に示すRAM型の記録媒体250のRAM領域251に書き込む。

【0300】なお、SAM3051内での処理のうち、コンテンツの購入形態が未決定のROM型の記録媒体の購入形態を決定する際のAV機器3602内での処理の流れ、AV機器3603において購入形態が未決定のR

102

OM型の記録媒体からセキュアコンテナ304を読み出してこれをAV機器3602に転送してRAM型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ310の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキーファイル内にプライスタグデータ312を格納する点を除いて、第1実施形態のSAM1051の場合と同じである。

【0301】次に、図32に示すEMDシステム300の全体動作について説明する。図52および図53は、EMDシステム300の全体動作のフローチャートである。ここでは、サービスプロバイダ310からユーザホームネットワーク303にオンラインでセキュアコンテナ304を送信する場合を例示して説明する。なお、以下に示す処理の前提として、EMDサービスセンタ302へのコンテンツプロバイダ301、サービスプロバイダ310およびSAM3051～3054の登録は既に終了しているものとする。

【0302】ステップS21：EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データKCP、Pの公開鍵証明書CERCPを、自らの署名データSIG1、ESCと共にコンテンツプロバイダ301に送信する。また、EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データKSP、Pの公開鍵証明書CERSPを、自らの署名データSIG61、ESCと共にサービスプロバイダ310に送信する。また、EMDサービスセンタ302は、各々有効期限が1カ月の6カ月分の配信用鍵データKD1～KD6をコンテンツプロバイダ301に送信し、3カ月分の配信用鍵データKD1～KD3をユーザホームネットワーク303のSAM3051～3054に送信する。

【0303】ステップS22：コンテンツプロバイダ301は、図6(A)に示す権利登録要求モジュールMod2を、EMDサービスセンタ302に送信する。そして、EMDサービスセンタ302は、所定の署名検証を行った後に、権利書データ106およびコンテンツ鍵データKcを登録して権威化(認証)する。

【0304】ステップS23：コンテンツプロバイダ301は、署名データの作成処理や、SIG対応する期間の配信用鍵データKD1～KD3などを用いた暗号化処理を経て、図4(A)、(B)、(C)に示すデータを格納したセキュアコンテナ104を、サービスプロバイダ310に供給する。

【0305】ステップS24：サービスプロバイダ310は、図4(C)に示す署名データSIG1、ESCを検証した後に、公開鍵証明書データCERCPに格納された公開鍵データKCP、Pを用いて、図4(A)、(B)に示す署名データSIG6、CPおよびSIG7、CPを検証して、セキュアコンテナ104が正当なコンテンツプロバイダ301から送信されたものであるかを確認する。

【0306】ステップS25：サービスプロバイダ31

103

0は、プライスタグデータ312を作成し、プライスタグデータ312を格納した図35に示すセキュアコンテナ304を作成する。

【0307】ステップS26：サービスプロバイダ310は、図37に示すプライスタグ登録要求モジュールMod102を、EMDサービスセンタ302に送信する。そして、EMDサービスセンタ302は、所定の署名検証を行った後に、プライスタグデータ312を登録して権威化する。

【0308】ステップS27：サービスプロバイダ310は、例えば、ユーザホームネットワーク303のCAモジュール311からの要求に応じて、ステップS25で作成したセキュアコンテナ304を、オンラインあるいはオフラインで、図42に示すネットワーク機器3601の復号モジュール905に送信する。

【0309】ステップS28：CAモジュール311は、SP用購入履歴データ309を作成し、これを所定のタイミングで、サービスプロバイダ310に送信する。

【0310】ステップS29：SAM305₁～305₄のいずれかにおいて、図35(D)に示す署名データSIG_{61,ESC}を検証した後に、公開鍵証明書データCER_{SP}に格納された公開鍵データK_{SP,P}を用いて、図35(A), (B), (C)に示す署名データSIG_{62,SP}、SIG_{63,SP}、SIG_{64,SP}を検証して、セキュアコンテナ304が正当なサービスプロバイダ310から送信されたものであるかを確認する。

【0311】ステップS30：SAM305₁～305₄のいずれかにおいて、配信用鍵データKD₁～KD₃を用いて、図35(B)に示すキーファイルKFを復号する。そして、SAM305₁～305₄のいずれかにおいて、図35(B)に示す署名データSIG_{1,ESC}を検証した後に、公開鍵証明書データCER_{CP}に格納された公開鍵データK_{CP,P}を用いて、図35(B)に示す署名データSIG_{2,CP}、SIG_{3,CP}およびSIG_{4,CP}を検証して、コンテンツデータC、コンテンツ鍵データK_Cおよび権利書データ106が正当なコンテンツプロバイダ301によって作成されたものであるかを確認する。

【0312】ステップS31：ユーザが図42の購入・利用形態決定操作部165を操作してコンテンツの購入・利用形態を決定する。

【0313】ステップS32：ステップS31において生成された操作信号S165に基づいて、SAM305₁～305₄において、セキュアコンテナ304の利用履歴(Usage Log)データ308が生成される。SAM305₁～305₄からEMDサービスセンタ302に、利用履歴データ308およびその署名データSIG205、SAM1が送信される。

【0314】EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301

104

およびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、決済請求権データ152c, 152sを作成する。

【0315】EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c, 152sを自らの署名データと共に送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310の所有者に分配される。

【0316】以上説明したように、EMDシステム300によれば、EMDサービスセンタ302が、認証機能、鍵データ管理機能および権利処理(利益分配)機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ301およびEMDサービスセンタ302の所有者に、予め決められた比率に従って確実に分配される。また、EMDシステム300によれば、同じコンテンツプロバイダ301が供給した同じコンテンツファイルCFについての権利書データ106は、サービスプロバイダ310のサービス形態とは無関係に、そのままSAM305₁～305₄に供給される。従って、SAM305₁～305₄において、権利書データ106に基づいて、コンテンツプロバイダ301の意向通りに、コンテンツファイルCFの利用を行わせることができる。すなわち、EMDシステム300によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織725に頼ることなく、技術的な手段によって、コンテンツプロバイダ301の所有者の権利および利益を確実に守ることができる。

【0317】第2実施形態の第1変形例

図54は、第2実施形態の第1変形例に係わる2個のサービスプロバイダを用いたEMDシステム300aの構成図である。図54において、図32と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。図54に示すように、EMDシステム300aでは、コンテンツプロバイダ301からサービスプロバイダ310aおよび310bに、同じセキュアコンテナ104を供給する。

【0318】サービスプロバイダ310aは、例えば、コンテンツをドラマ番組の提供サービスを行っており、当該サービスにおいて、当該ドラマ番組に関連するコンテンツデータCと、当該コンテンツデータCについて独自に作成したプライスタグデータ312aとを格納したセキュアコンテナ304aを作成し、これをネットワーク機器3601に配給する。また、サービスプロバイダ310bは、例えば、カラオケサービスを提供しており、当該サービスにおいて、当該カラオケサービスに関連するコンテンツデータCと、当該コンテンツデータCについて独自に作成したプライスタグデータ312bと

105

を格納したセキュアコンテナ304bを作成し、これをネットワーク機器360₁に配給する。ここで、セキュアコンテナ304a、304bのフォーマットは、図35を用いた説明したセキュアコンテナ304と同じである。

【0319】ネットワーク機器360_{a1}には、サービスプロバイダ310a、310bの各々に対応したCAモジュール311a、311bが設けられている。CAモジュール311a、311bは、自らの要求に応じたセキュアコンテナ304a、304bの配給を、それぞれサービスプロバイダ310a、310bから受ける。

【0320】次に、CAモジュール311a、311bは、配給されたセキュアコンテナ304a、304bに応じたSP用購入履歴データ309a、309bをそれぞれ作成し、これらをそれぞれサービスプロバイダ310a、310bに送信する。また、CAモジュール311a、311bは、セキュアコンテナ304a、304bをセッション鍵データK_{SES}で復号した後に、SAM305₁～305₄に出力する。

【0321】次に、SAM305₁～305₄において、共通の配信用鍵データKD₁～KD₃を用いて、セキュアコンテナ304a、304b内のキーファイルKFが復号され、共通の権利書データ106に基づいて、ユーザからの操作に応じたコンテンツの購入・利用に関する処理が行われ、それに応じた利用履歴データ308が作成される。

【0322】そして、SAM305₁～305₄からEMDサービスセンタ302に、利用履歴データ308が送信される。

【0323】EMDサービスセンタ302では、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310a、310bの各々について、課金内容を決定(計算)し、その結果に基づいて、それぞれに対応する決済請求権データ152c、152sa、152sbを作成する。

【0324】EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c、152sa、152sbを送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310a、310bの所有者に分配される。

【0325】上述したように、EMDシステム300bによれば、同じコンテンツファイルCFをサービスプロバイダに310a、310bに供給する場合に、当該コンテンツファイルCFについての権利書データ106を配信用鍵データKD₁～KD₆で暗号化してサービスプロバイダに310a、310bに供給し、サービスプロバイダに310a、310bは暗号化された権利書データ106をそのまま格納したセキュアコンテナ304

106

a、304bをユーザホームネットワークに配給する。そのため、ユーザホームネットワーク内のSAM305₁～305₄では、コンテンツファイルCFをサービスプロバイダに310a、310bの何れから配給を受けた場合でも、共通の権利書データ106に基づいて権利処理を行うことができる。

【0326】なお、上述した第1変形例では、2個のサービスプロバイダを用いた場合を例示したが、本発明では、サービスプロバイダの数は任意である。

10 【0327】第2実施形態の第2変形例

図55は、第2実施形態の第2変形例に係わる複数のコンテンツプロバイダを用いたEMDシステム300bの構成図である。図55において、図32と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。図55に示すように、EMDシステム300bでは、コンテンツプロバイダ301a、301bからサービスプロバイダ310に、それぞれセキュアコンテナ104a、104bが供給される。

【0328】サービスプロバイダ310は、例えば、コンテンツプロバイダ301a、301bが供給したコンテンツを用いてサービスを提供しており、セキュアコンテナ104aについてのプライスタグデータ312aと、セキュアコンテナ104bについてのプライスタグデータ312bとをそれぞれ生成し、これらを格納したセキュアコンテナ304cを作成する。図55に示すように、セキュアコンテナ304cには、コンテンツファイルCFa、CFb、キーファイルKFa、KFb、プライスタグデータ312a、312b、それらの各々についてのサービスプロバイダ310の秘密鍵データK_{CP, S}による署名データが格納されている。

【0329】セキュアコンテナ304cは、ユーザホームネットワーク303のネットワーク機器360₁のCAモジュール311で受信された後に、SAM305₁～305₄において処理される。

【0330】SAM305₁～305₄では、配信用鍵データKD_{a1}～KD_{a3}を用いて、キーファイルKFaが復号され、権利書データ106aに基づいて、コンテンツファイルCFaについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ308に記述される。また、SAM305₁～305₄において、配信用鍵データKD_{b1}～KD_{b3}を用いて、キーファイルKFbが復号され、権利書データ106bに基づいて、コンテンツファイルCFbについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ308に記述される。

【0331】そして、SAM305₁～305₄からEMDサービスセンタ302に、利用履歴データ308が送信される。

50 【0332】EMDサービスセンタ302では、利用履

107

歴データ308に基づいて、コンテンツプロバイダ301a, 301bおよびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、それぞれに対応する決済請求権データ152ca, 152cb, 152sを作成する。

【0333】EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152ca, 152cb, 152sを送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301a, 301bおよびサービスプロバイダ310の所有者に分配される。

【0334】上述したように、EMDシステム300bによれば、セキュアコンテナ304c内に格納されたコンテンツファイルCFa, CFbの権利書データ106a, 106bは、コンテンツプロバイダ301a, 301bが作成したものをそのまま用いるため、SAM3051~3054内において、権利書データ106a, 106bに基づいて、コンテンツファイルCFa, CFbについての権利処理がコンテンツプロバイダ301a, 301bの意向に沿って確実に行われる。

【0335】なお、図55に示す第2変形例では、2個のコンテンツプロバイダを用いた場合を例示したが、コンテンツプロバイダの数は任意である。また、コンテンツプロバイダおよびサービスプロバイダの双方が複数であってもよい。

【0336】第2実施形態の第3変形例

図56は、第2実施形態の第3変形例に係わるEMDシステムの構成図である。上述した第2実施形態では、EMDサービスセンタ302が決済機関91に対して、コンテンツプロバイダ301およびサービスプロバイダ310の決済を行う場合を例示したが、本発明では、例えば、図56に示すように、EMDサービスセンタ302において、利用履歴データ308に基づいて、コンテンツプロバイダ301のための決済請求権データ152cと、サービスプロバイダ310のための決済請求権データ152sとを作成し、これらをそれぞれコンテンツプロバイダ301およびサービスプロバイダ310に送信するようにしてもよい。この場合には、コンテンツプロバイダ301は、決済請求権データ152cを用いて、ペイメントゲートウェイ90aを介して決済機関91aに決済を行う。また、サービスプロバイダ310は、決済請求権データ152sを用いて、ペイメントゲートウェイ90bを介して決済機関91bに決済を行う。

【0337】第2実施形態の第4変形例

図57は、第2実施形態の第4変形例に係わるEMDシステムの構成図である。上述した第2実施形態では、例えば現行のインターネットのようにサービスプロバイダ310が課金機能を有していない場合を例示したが、現行のデジタル放送などのようにサービスプロバイダ31

108

0が課金機能を有している場合には、CAモジュール311において、セキュアコンテナ304に関するサービスプロバイダ310のサービスに対しての利用履歴データ308sを作成してサービスプロバイダ310に送信する。そして、サービスプロバイダ310は、利用履歴データ308sに基づいて、課金処理を行って決済請求権データ152sを作成し、これを用いてペイメントゲートウェイ90bを介して決済機関91bに決済を行う。一方、SAM3051~3054は、セキュアコンテナ304に関するコンテンツプロバイダ301の権利処理に対しての利用履歴データ308cを作成し、これをEMDサービスセンタ302に送信する。EMDサービスセンタ302は、利用履歴データ308cに基づいて、決済請求権データ152cを作成し、これをコンテンツプロバイダ301に送信する。コンテンツプロバイダ301は、決済請求権データ152cを用いて、ペイメントゲートウェイ90aを介して決済機関91aに決済を行う。

【0338】第2実施形態の第5変形例

上述した実施形態では、図40に示すように、EMDサービスセンタ302のユーザ嗜好フィルタ生成部901において、SAM3051などから受信した利用履歴データ308に基づいて、ユーザ嗜好フィルタデータ903を生成する場合を例示したが、例えば、図46に示すSAM3051などの利用監視部186で生成した利用制御状態データ166をリアルタイムでEMDサービスセンタ302に送信するようにして、SP用購入履歴データ309において、利用制御状態データ166に基づいてユーザ嗜好フィルタデータ903を生成するようにしてもよい。

【0339】第2実施形態の第6変形例

コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051~3054は、それぞれ自らの公開鍵データKcp,P, Ksp,P, KSAM1,P~KSAM4,Pの他に、自らの秘密鍵データKcp,S, Ksp,S, KSAM1,S~KSAM4,SをEMDサービスセンタ302に登録してもよい。このようにすることで、EMDサービスセンタ302は、緊急時に、国家あるいは警察機関などからの要請に応じて、秘密鍵データKcp,S, Ksp,S, KSAM1,S~KSAM4,Sを用いて、コンテンツプロバイダ301とサービスプロバイダ310との間の通信、サービスプロバイダ310とSAM3051~3054との間の通信、並びにユーザホームネットワーク303内でのSAM3051~3054相互間での通信のうち対象となる通信を盗聴することが可能になる。また、SAM3051~3054については、出荷時に、EMDサービスセンタ302によって秘密鍵データKSAM1,S~KSAM4,Sを生成し、これをSAM3051~3054に格納すると共にEMDサービスセンタ302が保持(登録)するようにしてもよい。

109

【0340】第2実施形態の第7変形例

上述した実施形態では、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051~3054が、相互に通信を行う場合に、EMDサービスセンタ302から事前に公開鍵証明書データCERCP, CERSP, CERSAM1~CERSAN4を取得し、イン・バンド方式で通信先に送信する場合を例示したが、本発明では、通信先への公開鍵証明書データの送信形態として種々の形態を採用できる。例えば、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051~3054が、相互に通信を行う場合に、EMDサービスセンタ302から事前に公開鍵証明書データCERCP, CERSP, CERSAM1~CERSAN4を取得し、当該通信に先立ってアウト・オブ・バンド方式で通信先に送信してもよい。また、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051~3054が、通信時に、EMDサービスセンタ302から公開鍵証明書データCERCP, CERSP, CERSAM1~CERSAN4を取得してもよい。

【0341】図58は、公開鍵証明書データの取得（入手）ルートの形態を説明するための図である。なお、図58において、図32と同じ符号を付した構成要素は、前述した同一符号の構成要素と同じである。また、ユーザホームネットワーク303aは、前述したユーザホームネットワーク303と同じである。ユーザホームネットワーク303bでは、IEEE1394シリアルバスであるバス191を介してSAM30511~30514を接続している。

【0342】コンテンツプロバイダ301がサービスプロバイダ310の公開鍵証明書データCERSPを取得する場合には、例えば、通信に先立ってサービスプロバイダ310からコンテンツプロバイダ301に公開鍵証明書データCERSPを送信する場合（図58中（3））と、コンテンツプロバイダ301がEMDサービスセンタ302から公開鍵証明書データCERSPを取り寄せる場合（図58中（1））とがある。

【0343】また、サービスプロバイダ310がコンテンツプロバイダ301の公開鍵証明書データCERCPを取得する場合には、例えば、通信に先立ってコンテンツプロバイダ301からサービスプロバイダ310に公開鍵証明書データCERCPを送信する場合（図58中（2））と、サービスプロバイダ310がEMDサービスセンタ302から公開鍵証明書データCERCPを取り寄せる場合（図58中（4））とがある。

【0344】また、サービスプロバイダ310がSAM3051~3054の公開鍵証明書データCERSAM1~CERSAM4を取得する場合には、例えば、通信に先立ってSAM3051~3054からサービスプロバイダ310に公開鍵証明書データCERSAM1~CERSAM4を送信する場合（図58中（6））と、サービスプロバイダ

110

310がEMDサービスセンタ302から公開鍵証明書データCERSAM1~CERSAM4を取り寄せる場合（図58中（4））とがある。

【0345】また、SAM3051~3054がサービスプロバイダ310の公開鍵証明書データCERSPを取得する場合には、例えば、通信に先立ってサービスプロバイダ310からSAM3051~3054に公開鍵証明書データCERSPを送信する場合（図58中（5））と、SAM3051~3054がEMDサービスセンタ302から公開鍵証明書データCERSPを取り寄せる場合（図58中（7）など）とがある。

【0346】また、SAM3051がSAM3052の公開鍵証明書データCERSAM2を取得する場合には、例えば、通信に先立ってSAM3052からSAM3051に公開鍵証明書データCERSAM2を送信する場合（図58中（8））と、SAM3051がEMDサービスセンタ302から公開鍵証明書データCERSAM2を取り寄せる場合（図58中（7）など）とがある。

【0347】また、SAM3052がSAM3051の公開鍵証明書データCERSAM1を取得する場合には、例えば、通信に先立ってSAM3051からSAM3052に公開鍵証明書データCERSAM1を送信する場合（図58中（9））と、SAM3052が自らEMDサービスセンタ302から公開鍵証明書データCERSAM1を取り寄せる場合と、SAM3051が搭載されたネットワーク機器を介して公開鍵証明書データCERSAM1を取り寄せる場合（図58中（7）、（8））とがある。

【0348】また、SAM3054がSAM30513の公開鍵証明書データCERSAM13を取得する場合には、例えば、通信に先立ってSAM30513からSAM3054に公開鍵証明書データCERSAM13を送信する場合（図58中（12））と、SAM3054が自らEMDサービスセンタ302から公開鍵証明書データCERSAM13を取り寄せる場合（図58中（10））と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データCERSAM13を取り寄せる場合とがある。

【0349】また、SAM30513がSAM3054の公開鍵証明書データCERSAM4を取得する場合には、例えば、通信に先立ってSAM3054からSAM30513に公開鍵証明書データCERSAM4を送信する場合（図58中（11））と、SAM30513が自らEMDサービスセンタ302から公開鍵証明書データCERSAM4を取り寄せる場合（図58中（13））と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データCERSAM4を取り寄せる場合とがある。

【0350】第2実施形態における公開鍵証明書破棄リスト（データ）の取り扱い

第2実施形態では、EMDサービスセンタ302におい

111

て、不正行為などに用いられたコンテンツプロバイダ301、サービスプロバイダ310およびSAM3051~3054が他の装置と通信できないようにするために、当該不正行為に用いられた装置の公開鍵証明書データを無効にする公開鍵証明書破棄データを作成する。そして、当該公開鍵証明書破棄データCRL(Certificate Revocation List)を、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051~3054に送信する。なお、公開鍵証明書破棄データCRLは、EMDサービスセンタ302の他に、例えば、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051~3054において生成してもよい。

【0351】先ず、EMDサービスセンタ302が、コンテンツプロバイダ301の公開鍵証明書データCERCPを無効にする場合について説明する。図59に示すように、EMDサービスセンタ302は、公開鍵証明書データCERCPを無効にすることを示す公開鍵証明書破棄データCRL1をサービスプロバイダ310に送信する(図59中(1))。サービスプロバイダ310は、コンテンツプロバイダ301から入力した署名データを検証する際に、公開鍵証明書破棄データCRL1を参照して公開鍵証明書データCERCPの有効性を判断し、有効であると判断した場合に公開鍵データKCP,Pを用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにコンテンツプロバイダ301からのデータを無効にする。なお、データを無効にするのではなく、通信を拒絶するようにしてもよい。

【0352】また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL1を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM3051に送信する(図59中(1)、(2))。SAM3051は、サービスプロバイダ310から入力したセキュアコンテナ内に格納されたコンテンツプロバイダ301の署名データを検証する際に、公開鍵証明書破棄データCRL1を参照して公開鍵証明書データCERCPの有効性を判断し、有効であると判断した場合に公開鍵データKCP,Pを用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。なお、EMDサービスセンタ302は、公開鍵証明書破棄データCRL1を、ユーザホームネットワーク303内のネットワーク機器を介してSAM3051に直接送信してもよい(図59中(3))。

【0353】次に、EMDサービスセンタ302が、サービスプロバイダ310の公開鍵証明書データCERSPを無効にする場合について説明する。図60に示すように、EMDサービスセンタ302は、公開鍵証明書データCERSPを無効にすることを示す公開鍵証明書破棄デ

112

ータCRL2をコンテンツプロバイダ301に送信する(図60中(1))。コンテンツプロバイダ301は、サービスプロバイダ310から入力した署名データを検証する際に、公開鍵証明書破棄データCRL2を参照して公開鍵証明書データCERSPの有効性を判断し、有効であると判断した場合に公開鍵データKSP,Pを用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにサービスプロバイダ310からのデータを無効にする。

【0354】また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL2を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM3051に送信する(図60中(2))。SAM3051は、サービスプロバイダ310から入力したセキュアコンテナ内に格納されたサービスプロバイダ310の署名データを検証する際に、公開鍵証明書破棄データCRL2を参照して公開鍵証明書データCERSPの有効性を判断し、有効であると判断した場合に公開鍵データKSP,Pを用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データCRL2の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データCRL2は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要がある。なお、EMDサービスセンタ302は、公開鍵証明書破棄データCRL2を、ユーザホームネットワーク303内のネットワーク機器を介してSAM3051に直接送信してもよい(図60中(3))。

【0355】次に、EMDサービスセンタ302が、例えばSAM3052の公開鍵証明書データCER_{SAM2}を無効にする場合について説明する。図61に示すように、EMDサービスセンタ302は、公開鍵証明書データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL3をコンテンツプロバイダ301に送信する(図61中(1))。コンテンツプロバイダ301は、公開鍵証明書破棄データCRL3をサービスプロバイダ310に送信する。サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM3051に公開鍵証明書破棄データCRL_{SAM1}を送信する(図61中(1))。SAM3051は、SAM3052から入力したデータに付加されたSAM3052の署名データを検証する際に、公開鍵証明書破棄データCRL3を参照して公開鍵証明書データCER_{SAM2}の有効性を判断し、有効であると判断した場合に公開鍵データK_{SAM2,P}を用いた署名検証を行い、無

効であると判断した場合に当該署名検証を行わずに当該データを無効にする。この場合に、サービスプロバイダ310において、公開鍵証明書破棄データCRL₃の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310において、公開鍵証明書破棄データCRL₃は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要がある。

【0356】EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310を介してSAM305₁に送信してもよい（図61中（1）、（2））。また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を、ユーザホームネットワーク303内のネットワーク機器を介してSAM305₁に直接送信してもよい（図61中（3））。

【0357】また、EMDサービスセンタ302は、例えばSAM305₂の公開鍵証明書データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL₃を作成し、これを保管する。また、ユーザホームネットワーク303は、バス191に接続されているSAMのSAM登録リストSRLを作成し、これをEMDサービスセンタ302に送信する（図62中（1））。EMDサービスセンタ302は、SAM登録リストに示されるSAM305₁～305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM（例えばSAM305₂）を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定して新たなSAM登録リストSRLを作成する。次に、EMDサービスセンタ302は、当該生成したSAM登録リストSRLをSAM305₁に送信する（図62中（1））。SAM305₁は、他のSAMと通信を行う際に、SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【0358】また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を作成し、これをコンテンツプロバイダ301に送信する（図62中（2））。コンテンツプロバイダ301は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310に送信する（図62中（2））。次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₃をSAM305₁に送信する（図62中（2））。SAM305₁は、自らが作成したSAM登録リストに示されるSAM305₁～305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM（例えばSAM305₂）を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。以後、SAM305₁は、他のSAMと通信を行う際に、当該SAM登録リストS

RLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【0359】また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を作成し、これをサービスプロバイダ310に送信する（図62中（3））。次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₃をSAM305₁に送信する（図62中（3））。SAM305₁は、自らが作成したSAM登録リストに示されるSAM305₁～305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM（例えばSAM305₂）を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。以後、SAM305₁は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【0360】EMDサービスセンタ302の役割等

図63は、図32に示すEMDサービスセンタ（クリアリングハウス）302の機能を権利管理用クリアリングハウス950と、電子決済用クリアリングハウス951とに分割した場合のEMDシステムの構成図である。当該EMDシステムでは、電子決済用クリアリングハウス951において、ユーザホームネットワーク303a、303bのSAMからの利用履歴データ308に基づいて、決済処理（利益分配処理）を行い、コンテンツプロバイダ301およびサービスプロバイダ310の決済請求権データをそれぞれ生成し、ペイメントゲートウェイ90を介して決済機関91において決済を行う。

【0361】また、権利管理用クリアリングハウス950は、電子決済用クリアリングハウス951からの決済通知に応じたコンテンツプロバイダ301およびサービスプロバイダ310の決済レポートを作成し、それらをコンテンツプロバイダ301およびコンテンツプロバイダ301に送信する。また、コンテンツプロバイダ301の権利書データ106およびコンテンツ鍵データKcの登録（権威化）などを行う。なお、図64に示すように、権利管理用クリアリングハウス950と電子決済用クリアリングハウス951とを単体の装置内に収納すると、図32に示すEMDサービスセンタ302となる。

【0362】また、本発明は、例えば、図65に示すように、EMDサービスセンタ302に、権利管理用クリアリングハウス960の機能を設け、権利管理用クリアリングハウス960において、権利書データ106の登録などを行うと共に、SAMからの利用履歴データ308に基づいてサービスプロバイダ310の決済請求権データを作成し、これをサービスプロバイダ310に送信してもよい。この場合には、サービスプロバイダ310は、自らの課金システムを電子決済用クリアリングハウ

115

ス961として利用し、権利管理用クリアリングハウス960からの決済請求権データに基づいて決済を行う。

【0363】また、本発明は、例えば、図66に示すように、EMDサービスセンタ302に、権利管理用クリアリングハウス970の機能を設け、権利管理用クリアリングハウス970において、権利書データ106の登録などを行うと共に、SAMからの利用履歴データ308に基づいてコンテンツプロバイダ301の決済請求権データを作成し、これをコンテンツプロバイダ301に送信してもよい。この場合には、コンテンツプロバイダ301は、自らの課金システムを電子決済用クリアリングハウス961として利用し、権利管理用クリアリングハウス970からの決済請求権データに基づいて決済を行う。

【0364】

【発明の効果】以上説明したように、本発明のデータ提供システムおよびその方法、管理装置並びにデータ処理装置によれば、データ処理装置においてデータ提供装置が提供した権利書データに基づいてコンテンツデータの利用が行われるため、データ提供装置の関係者の利益が適切に保護される。また、本発明のデータ提供システムおよびその方法と管理装置によれば、管理装置において権利書データなどの証明を行うため、例えば、権利書データなどが不正に改竄された場合などに適切に対処できる。また、本発明のデータ提供システムおよびその方法と管理装置によれば、データ提供装置の関係者の利益を保護するための監査の負担を軽減できる。

【図面の簡単な説明】

【図1】図1は、本発明の第1実施形態のEMDシステムの全体構成図である。

【図2】図2は、図1に示すコンテンツプロバイダの機能ブロック図であり、ユーザホームネットワークのSAMとの間で送受信されるデータに関連するデータの流れを示す図である。

【図3】図3は、図1に示すコンテンツプロバイダの機能ブロック図であり、コンテンツプロバイダとEMDサービスセンタとの間で送受信されるデータに関連するデータの流れを示す図である。

【図4】図4は、図1に示すコンテンツプロバイダからSAMに送信されるセキュアコンテンツのフォーマットを説明するための図である。

【図5】図5は、ROM型の記録媒体を説明するための図である。

【図6】図6(A)はコンテンツプロバイダからEMDサービスセンタに送信される権利登録要求用モジュールのフォーマットを説明するための図、図6(B)はEMDサービスセンタからコンテンツプロバイダに送信される権利化証明書モジュールを説明するための図である。

【図7】図7は、図1に示すEMDサービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送

116

受信されるデータに関連するデータの流れを示す図である。

【図8】図8は、図1に示すEMDサービスセンタの機能ブロック図であり、SAMおよび図1に示す決済機関との間で送受信されるデータに関連するデータの流れを示す図である。

【図9】図9は、図1に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図10】図10は、図1に示すユーザホームネットワーク内のSAMの機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテンツを復号するまでのデータの流れを示す図である。

【図11】図11は、図9に示す外部メモリに記憶されるデータを説明するための図である。

【図12】図12は、スタックメモリに記憶されるデータを説明するための図である。

【図13】図13は、図1に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図14】図14は、図10に示す記憶部に記憶されるデータを説明するための図である。

【図15】図15は、図1に示すユーザホームネットワーク内のSAMの機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

【図16】図16は、図9に示すネットワーク機器のダウンロードメモリにダウンロードされた既に入形態が決定されたコンテンツファイルを、AV機器のSAMに転送する場合の転送元のSAM内での処理の流れを説明するための図である。

【図17】図17は、図16に示す場合における転送元のSAM内でのデータの流れを示す図である。

【図18】図18は、購入形態が決定したセキュアコンテンツのフォーマットを説明するための図である。

【図19】図19は、図16に示す場合において、転送先のSAMにおいて、入力したコンテンツファイルなどを、RAM型あるいはROM型の記録媒体(メディア)に書き込む際のデータの流れを示す図である。

【図20】図20、コンテンツの購入形態が未決定の図5に示すROM型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV機器において購入形態を決定する際の処理の流れを説明するための図である。

【図21】図21は、図20に示す場合において、SAM内でのデータの流れを示す図である。

【図22】図22は、ユーザホームネットワーク内のAV機器において購入形態が未決定のROM型の記録媒体からセキュアコンテンツを読み出して、これを他のAV機器に転送してRAM型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図23】図23は、図22に示す場合における転送元

117

のSAM内でのデータの流れを示す図である。

【図24】図24は、図22に示す場合における転送先のSAM内でのデータの流れを示す図である。

【図25】図25は、図1に示すコンテンツプロバイダ、EMDサービスセンタおよびSAMの相互間で、イン・バンド方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図26】図26は、図1に示すコンテンツプロバイダ、EMDサービスセンタおよびSAMの相互間で、イン・バンド方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図27】図27は、バス191への機器の接続形態の一例を説明するための図である。

【図28】図28は、SAM登録リストのデータフォーマットを説明するための図である。

【図29】図29は、図1に示すコンテンツプロバイダの全体動作のフローチャートである。

【図30】本発明の第1実施形態の第2変形例を説明するための図である。

【図31】本発明の第1実施形態の第3変形例を説明するための図である。

【図32】図32は、本発明の第2実施形態のEMDシステムの全体構成図である。

【図33】図33は、図32に示すコンテンツプロバイダの機能ブロック図であり、サービスプロバイダに送信されるセキュアコンテナに関するデータの流れを示す図である。

【図34】図34は、図32に示すサービスプロバイダの機能ブロック図であり、ユーザホームネットワークとの間で送受信されるデータの流れを示す図である。

【図35】図35は、図32に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図36】図36は、図32に示すサービスプロバイダの機能ブロック図であり、EMDサービスセンタとの間で送受信されるデータの流れを示す図である。

【図37】図37は、サービスプロバイダからEMDサービスセンタに送信されるプライスタグ登録要求用モジュールのフォーマットを説明するための図である。

【図38】図38は、図32に示すEMDサービスセンタの機能ブロック図であり、サービスプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図39】図39は、図32に示すEMDサービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図40】図40は、図32に示すEMDサービスセンタの機能ブロック図であり、SAMとの間で送受信されるデータに関連するデータの流れを示す図である。

118

【図41】図41は、利用履歴データの内容を説明するための図である。

【図42】図42は、図32に示すネットワーク機器の構成図である。

【図43】図43は、図42に示すCAモジュールの機能ブロック図である。

【図44】図44は、図42に示すSAMの機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図45】図45は、図44に示す記憶部に記憶されるデータを説明するための図である。

【図46】図46は、図42に示すSAMの機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図47】図47は、購入形態が決定された後のキーファイルのフォーマットを説明するための図である。

【図48】図48は、図42に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV機器のSAMに転送する場合の転送先のSAM内での処理の流れを説明するための図である。

【図49】図49は、図48に示す場合の転送元のSAM内でのデータの流れを示す図である。

【図50】図50は、ネットワーク機器のSAMからAV機器のSAMに転送される購入形態が既に決定されたセキュアコンテナのフォーマットを説明するための図である。

【図51】図51は、図48に示す場合の転送先のSAM内でのデータの流れを示す図である。

【図52】図52は、図32に示すEMDシステムの全体動作のフローチャートである。

【図53】図53は、図32に示すEMDシステムの全体動作のフローチャートである。

【図54】図54は、本発明の第2実施形態の第1変形例に係わる2個のサービスプロバイダを用いたEMDシステムの構成図である。

【図55】図55は、本発明の第2実施形態の第2変形例に係わる複数のコンテンツプロバイダを用いたEMDシステムの構成図である。

【図56】図56は、本発明の第2実施形態の第3変形例に係わるEMDシステムの構成図である。

【図57】図57は、本発明の第2実施形態の第4変形例に係わるEMDシステムの構成図である。

【図58】図58は、公開鍵証明書データの取得ルートの形態を説明するための図である。

【図59】図59は、コンテンツプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図60】図60は、サービスプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図で

119

ある。

【図61】図61は、SAMの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図62】図62は、SAMの公開鍵証明書データを無効にする場合のその他の処理を説明するための図である。

【図63】図63は、図32に示すEMDシステムにおいて、EMDサービスセンタの代わりに権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを設けた場合を説明するための図である。

【図64】図64は、図63に示す権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを単体のEMDサービスセンタ内に設けた場合のEMDシステムの構成図である。

【図65】図65は、サービスプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合のEMDシステムの構成図である。

【図66】図66は、コンテンツプロバイダが電子決済 *

120

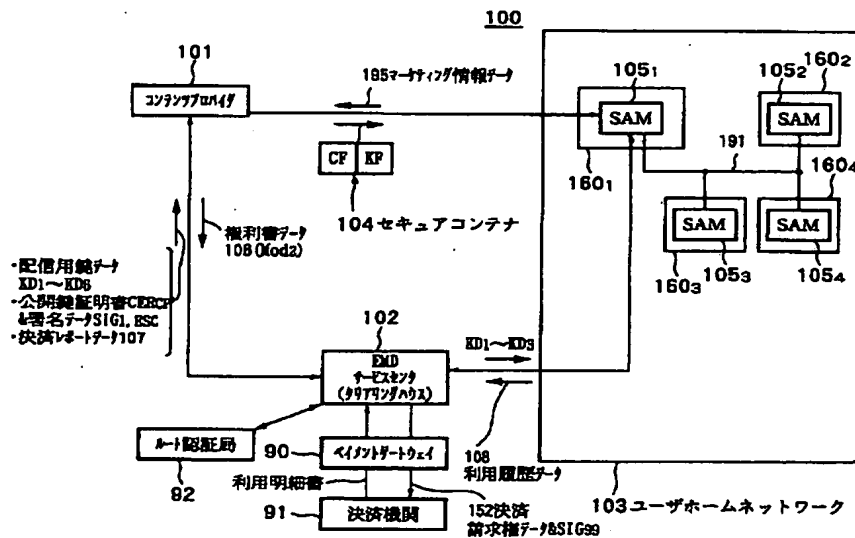
*用クリアリングハウスに直接的に決済を行う場合のEMDシステムの構成図である。

【図67】従来のEMDシステムの構成図である。

【符号の説明】

90…ペイメントゲートウェイ、91…決済機関、92…ルート認証局、100、300…EMDシステム、101、301…コンテンツプロバイダ、102、302…EMDサービスセンタ、103、303…ユーザホームネットワーク、104、304…セキュアコンテナ、105₁～105₄、305₁～305₄…SAM、106…権利書データ、107、307…決済レポートデータ、108、308…利用履歴データ、160₁…ネットワーク機器、160₂～160₄…AV機器、152、152c、152s…決済請求権データ、191…バス、310…サービスプロバイダ、311…CAモジュール、312…プライスタグデータ、CF…コンテンツファイル、KF…キーファイル、Kc…コンテンツ鍵データ

【図1】

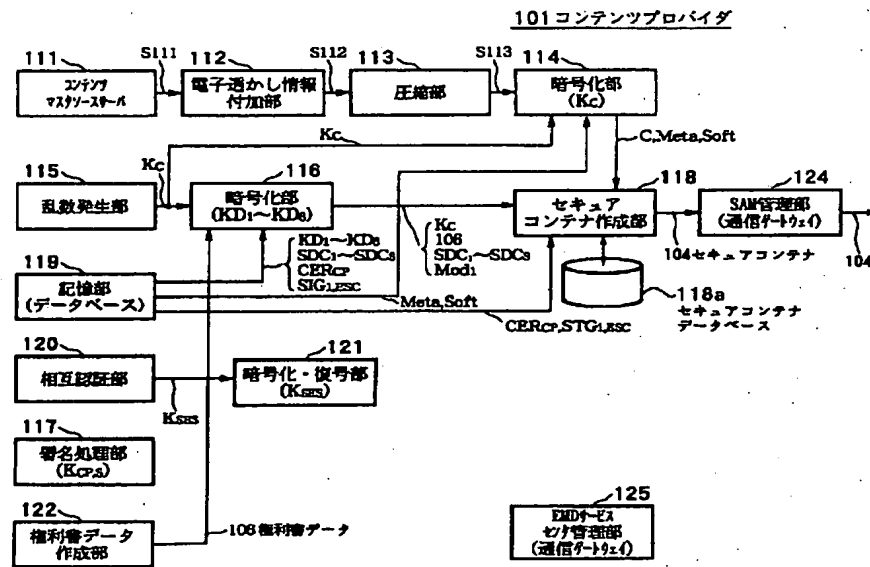


【図11】

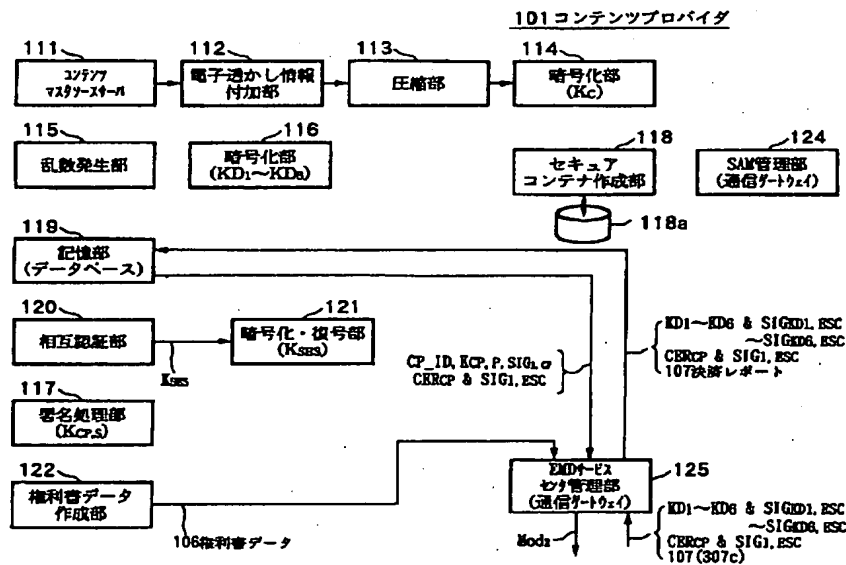
外装メモリ201に記憶されるデータ

利用履歴データ108
SAM登録リスト

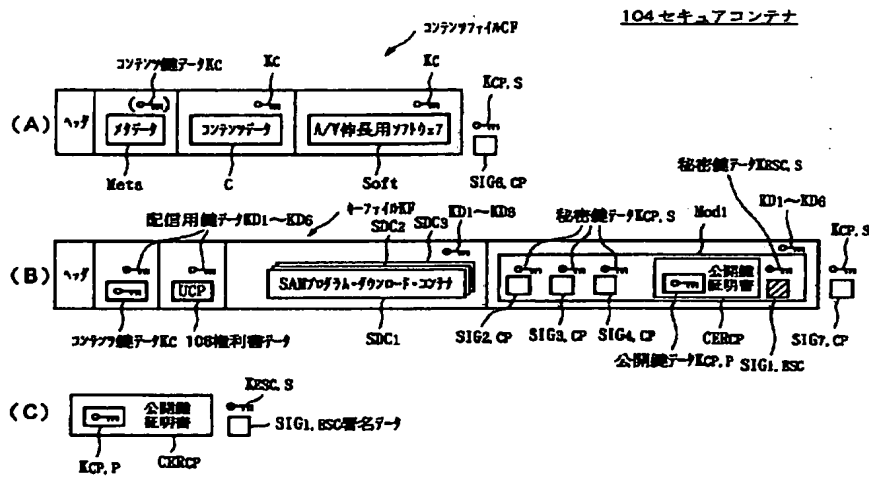
【図2】



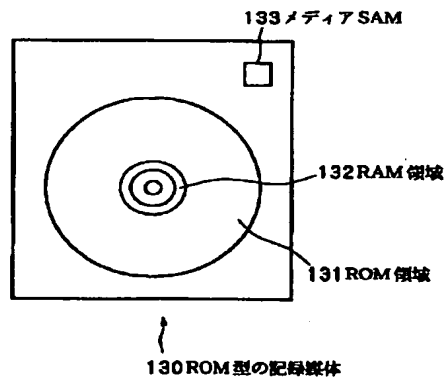
【図3】



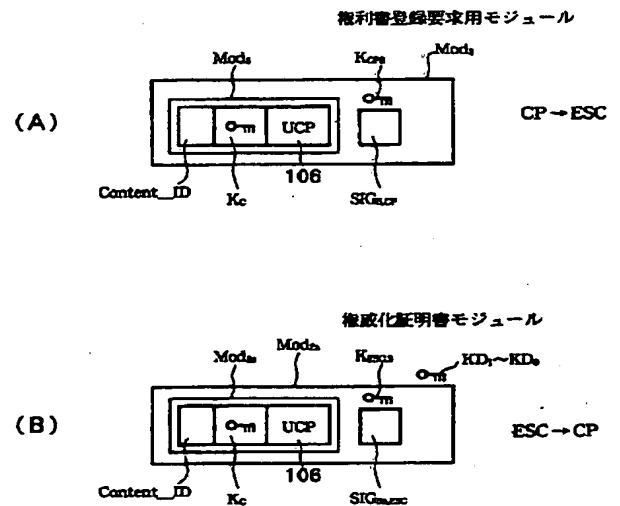
【図4】



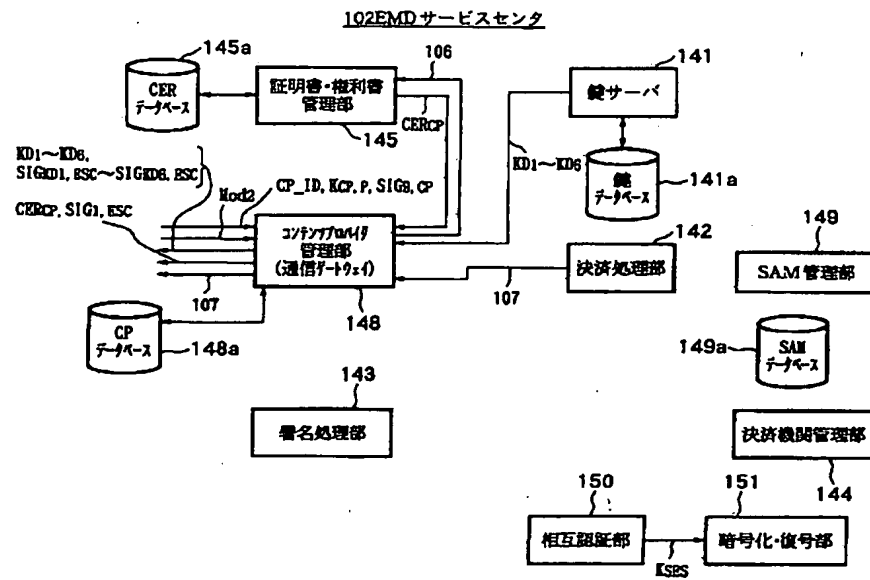
【図5】



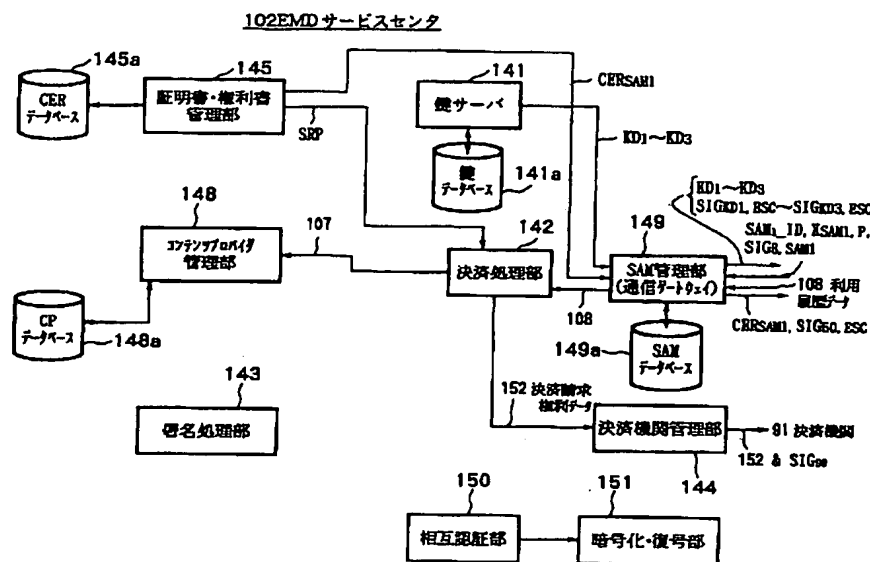
【図6】



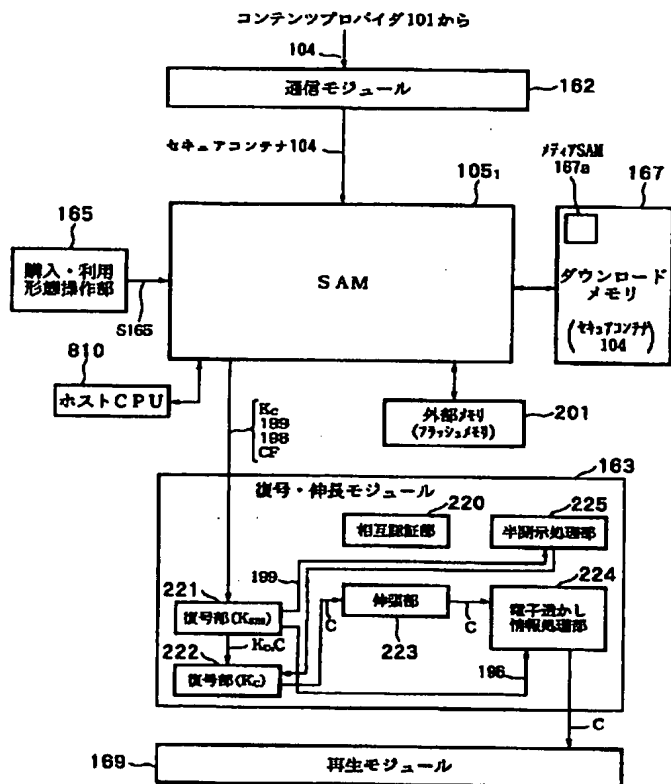
【図7】



【図8】



【図9】

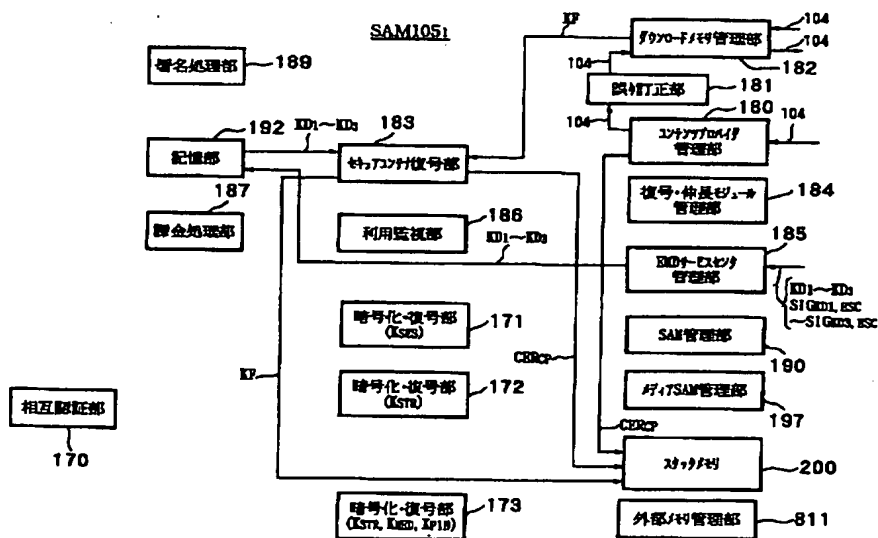


【図12】

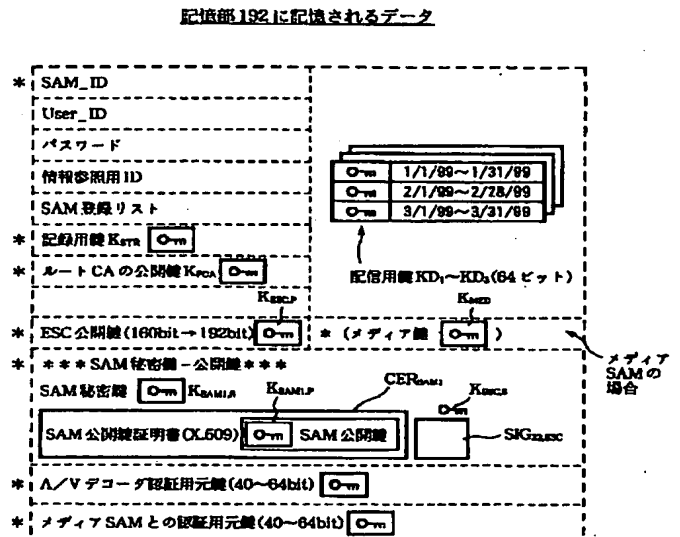
スタックメモリ200に記憶されるデータ

- 1 コンテンツ鍵データ Kc
- 権利者データ (UCP) 106
- 記憶部 (フラッシュメモリ) 192のロック鍵データ KLoc
- コンテンツプロバイダ101の公開鍵証明書 CERcp
- 利用制御状態データ (UCS) 166
- SAMプログラム・ダウンロード・コンテナSD₁~SD₃

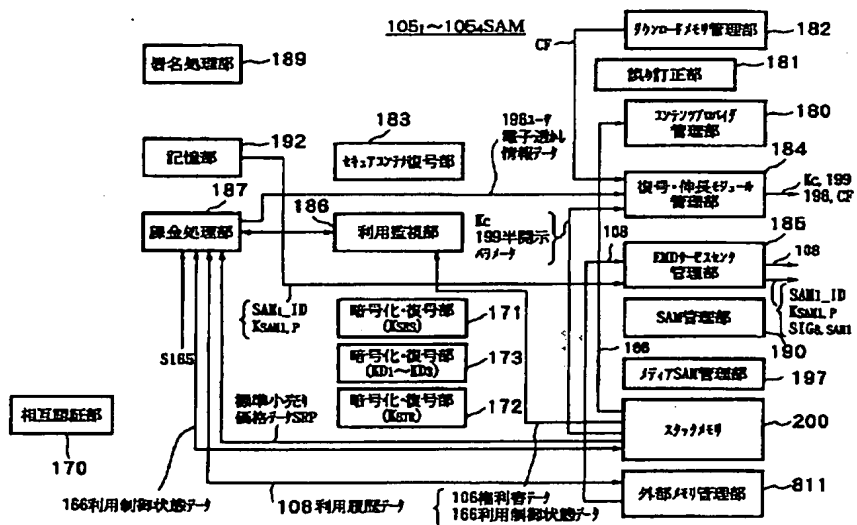
【図10】



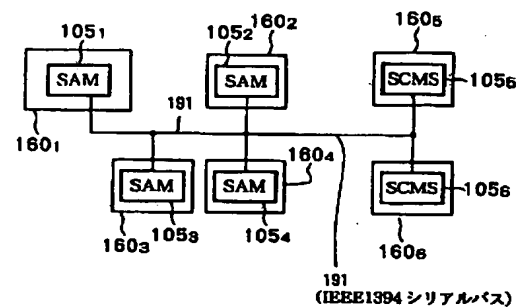
【图 14】



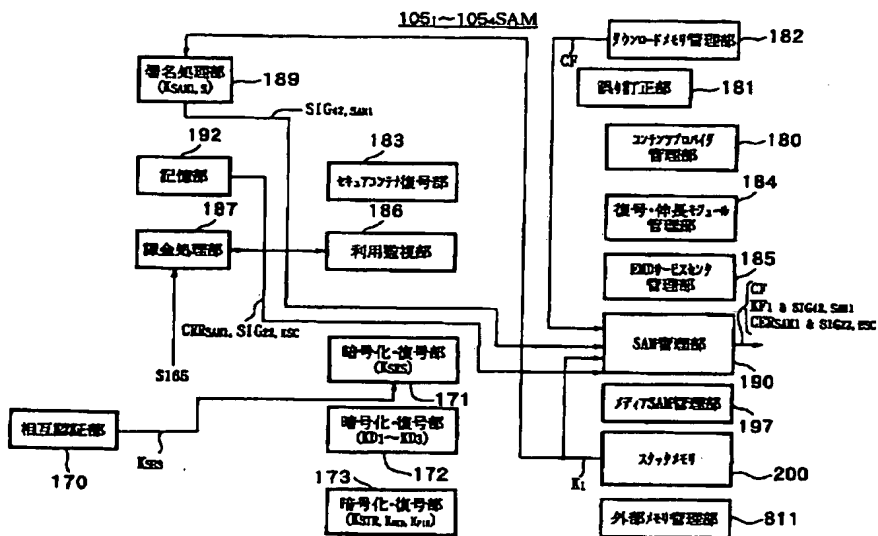
【圖 15】



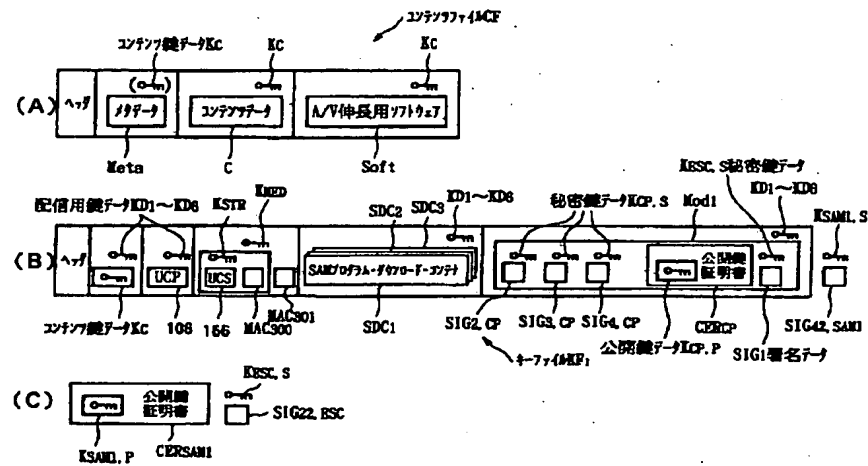
【图 2 7】



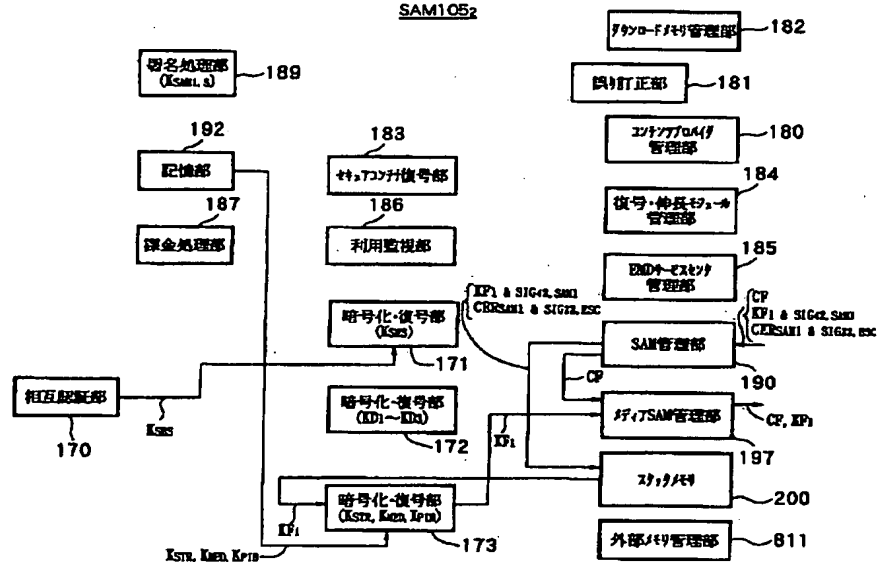
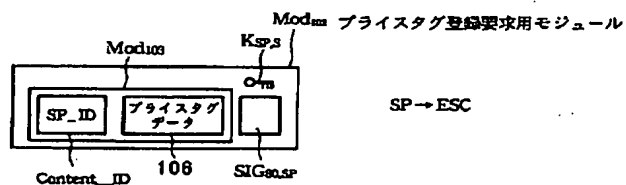
【图 17】



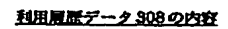
購入形態が決定したセキュアコンテナ



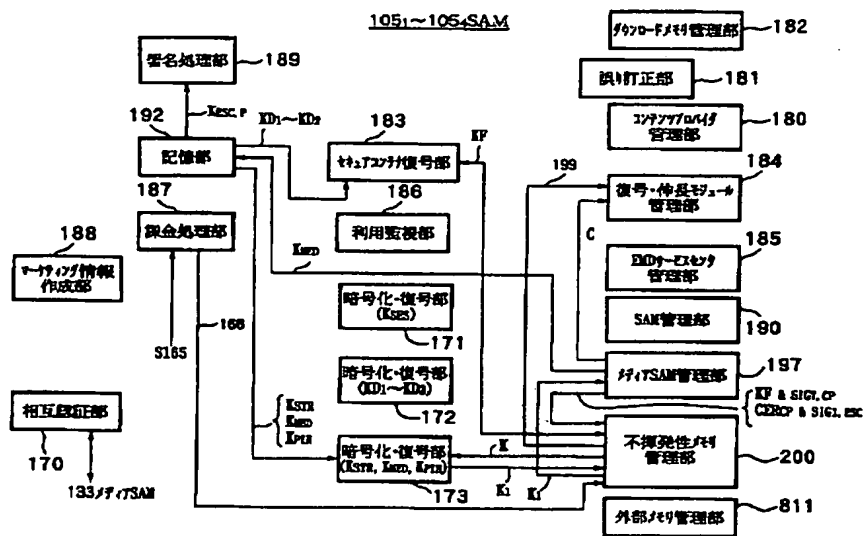
SAM1052

Mod_{ms} プライスタグ登録要求用モジュール

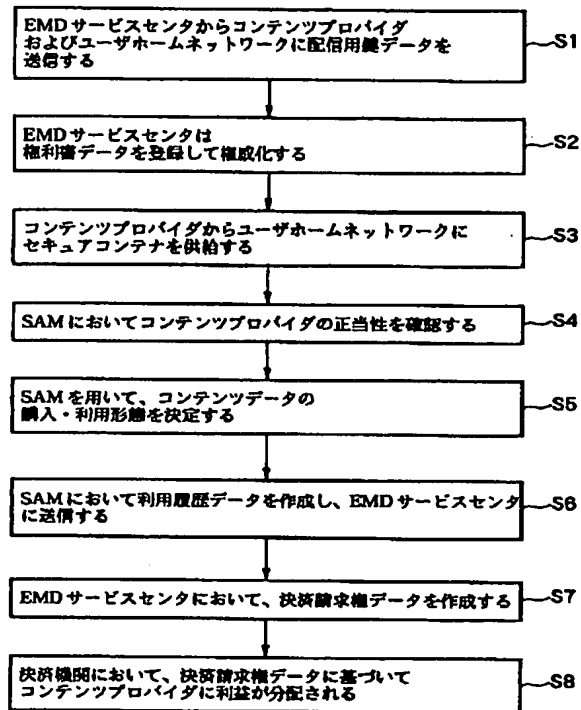
【图 4 1】



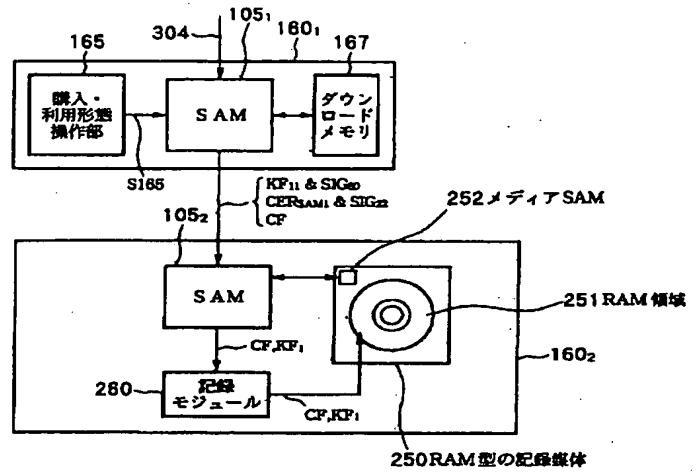
【図 2 1】



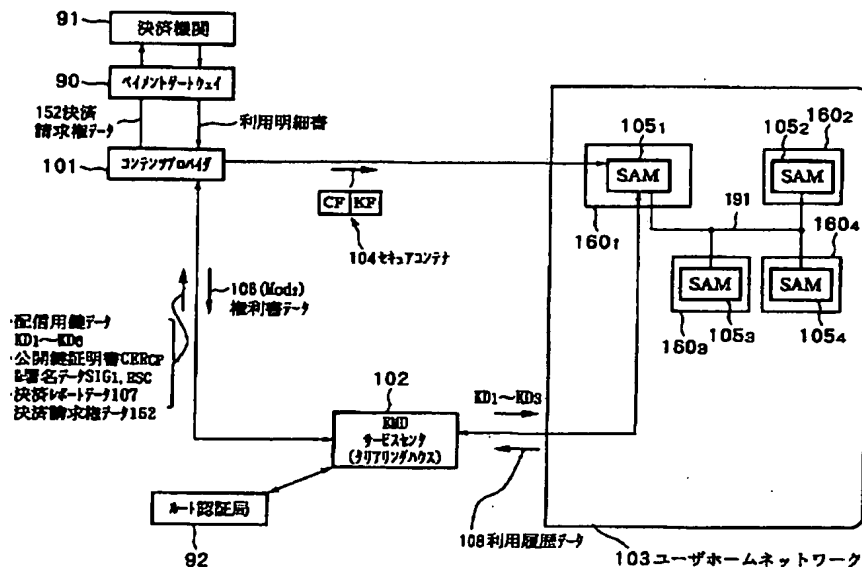
【圖 29】



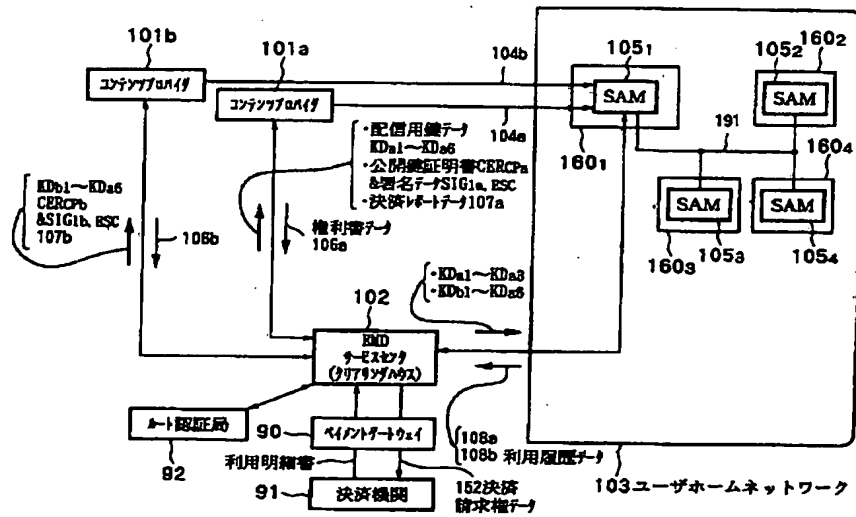
【図 4 8】



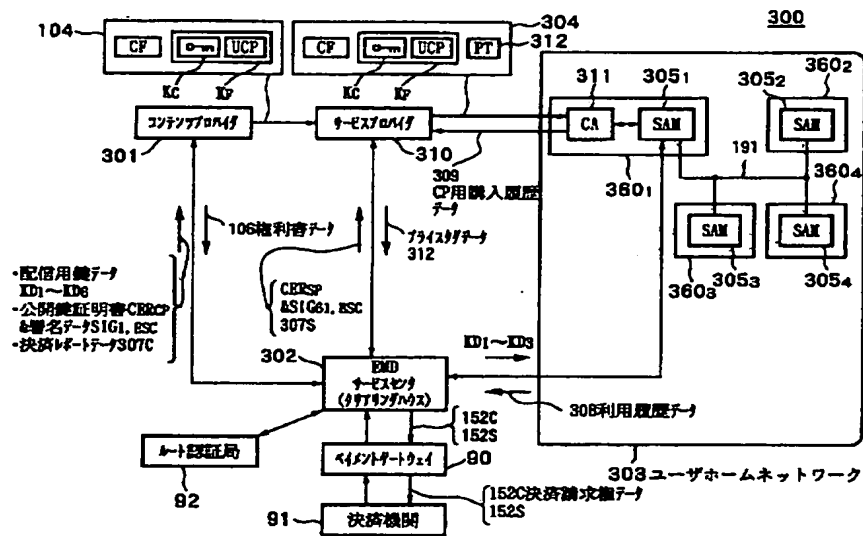
【図 30】



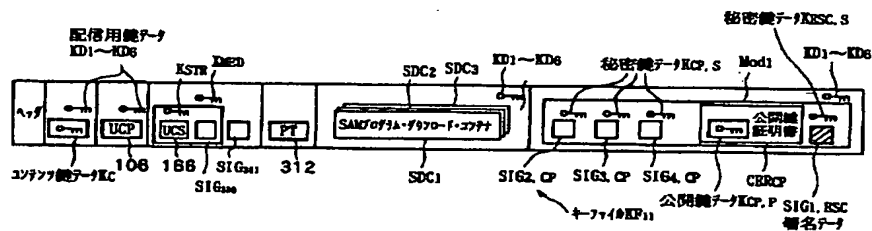
【図31】



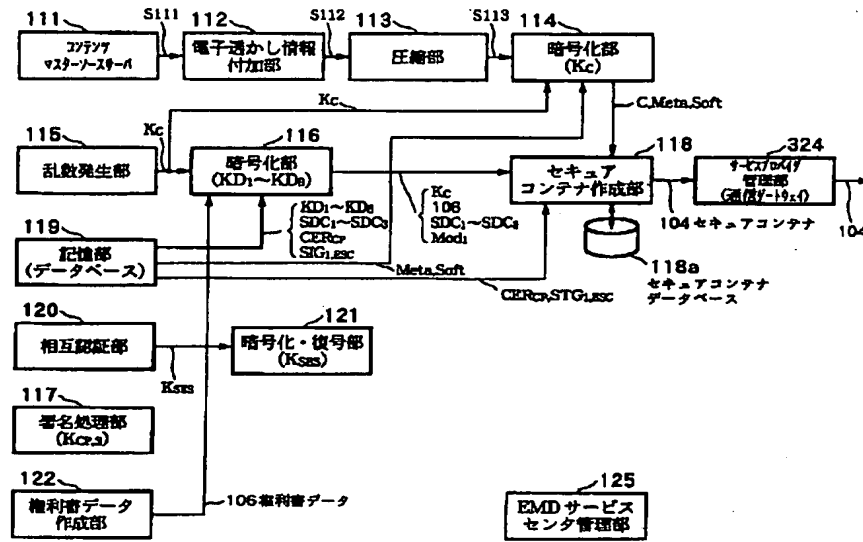
【図32】



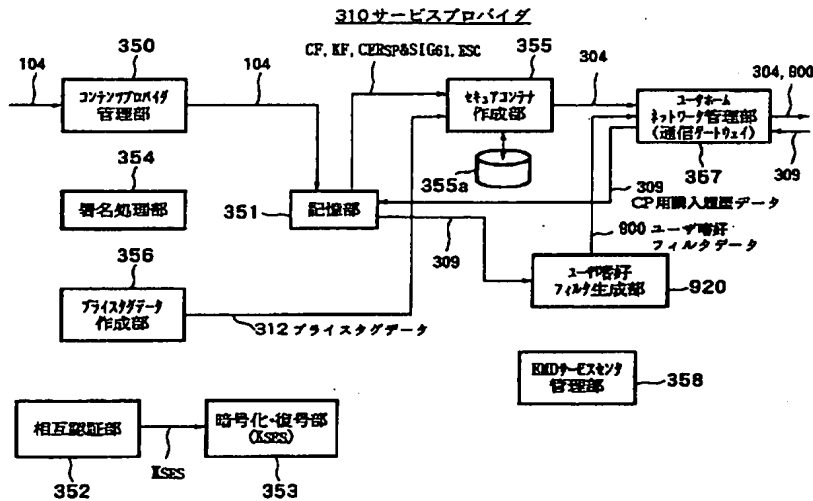
【図47】



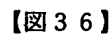
301 コンテンツプロバイダ



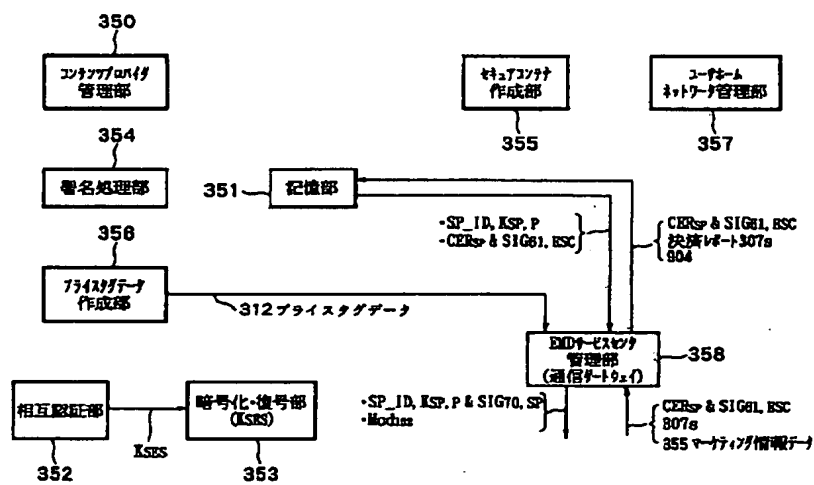
310 サービスプロバイダ



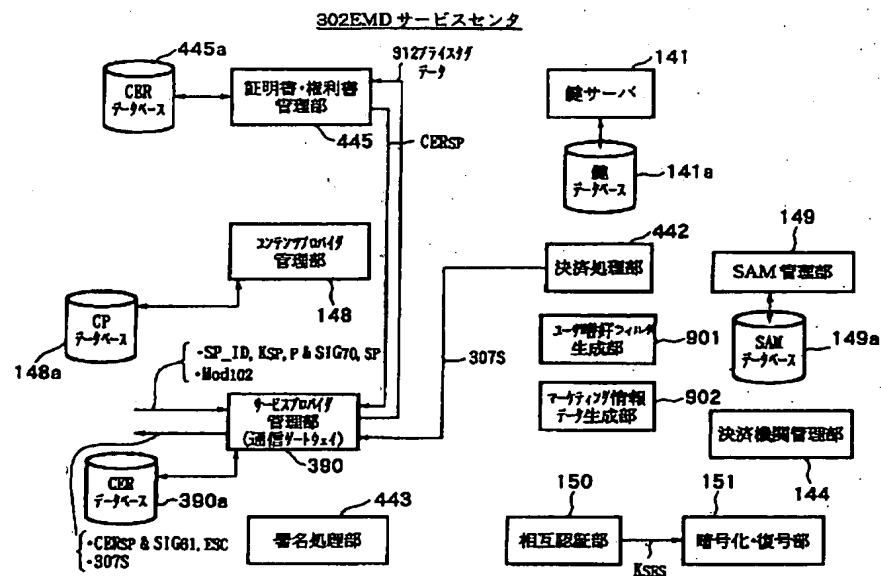
304 セキュアコンテナ



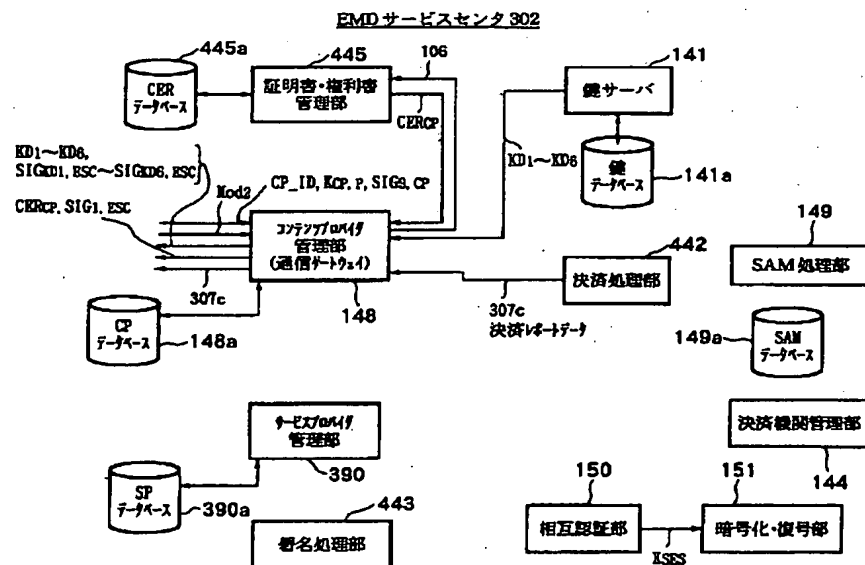
310 サービスプロバイダ



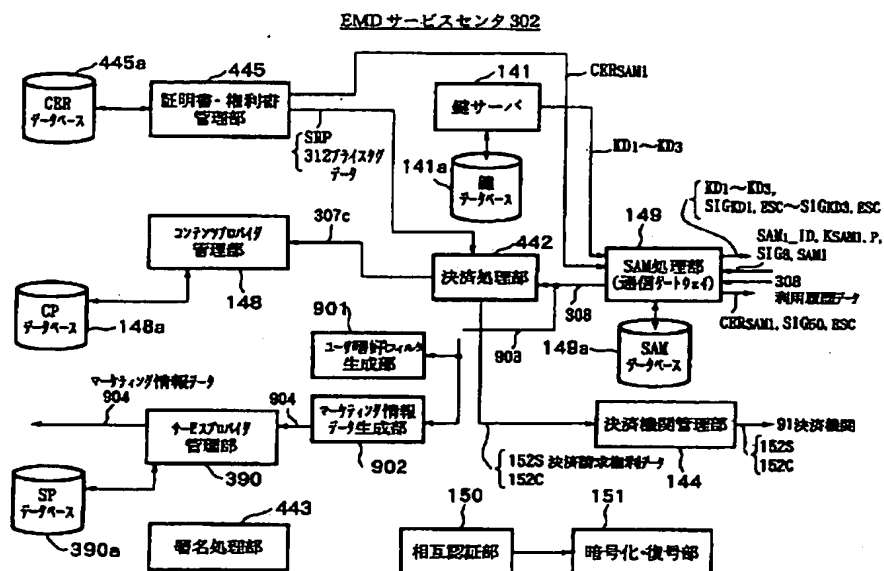
【図38】



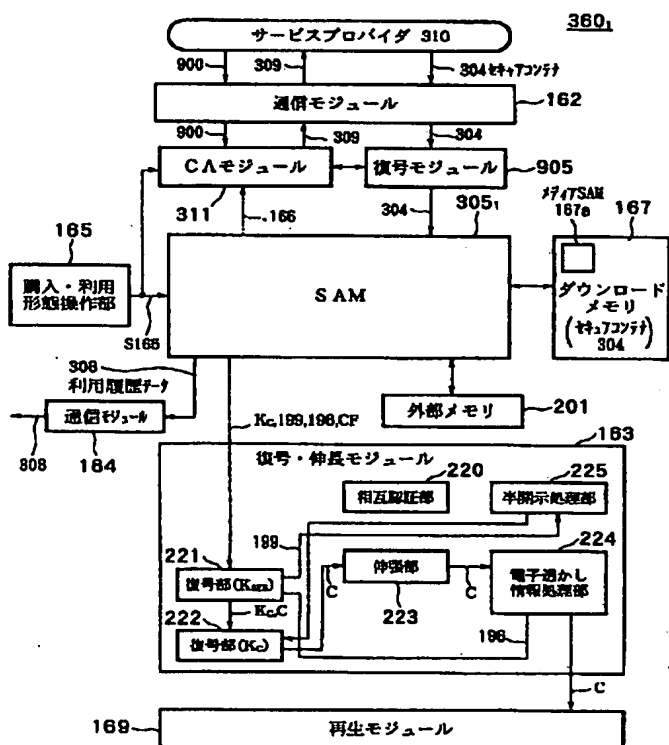
【図39】



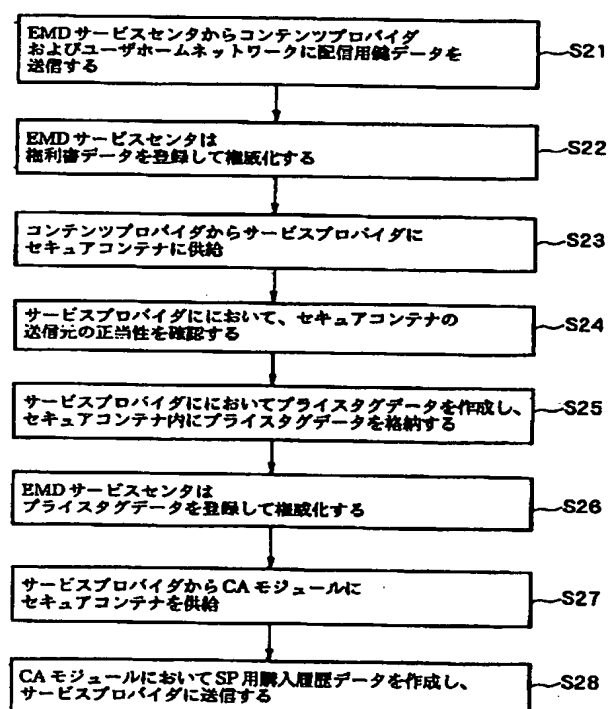
【图 40】



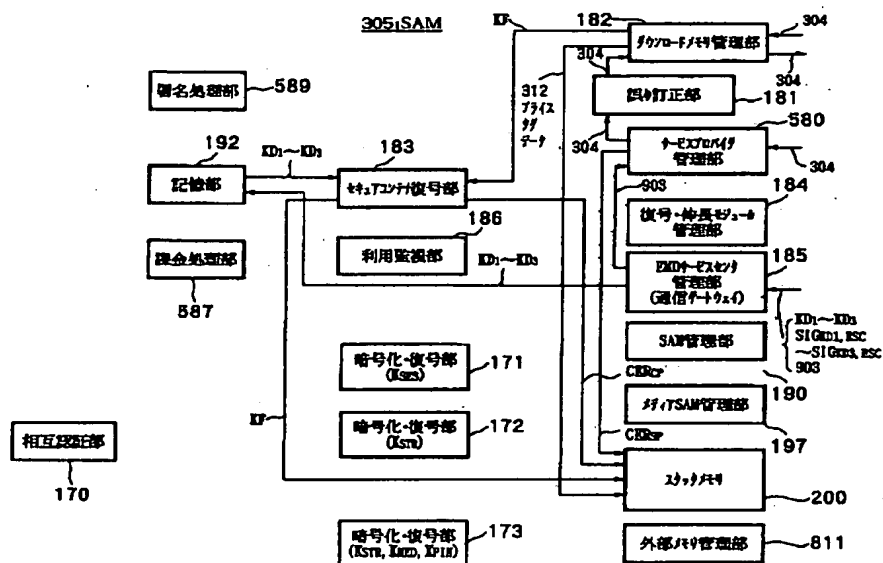
【图 4 2】



【图 5 2】

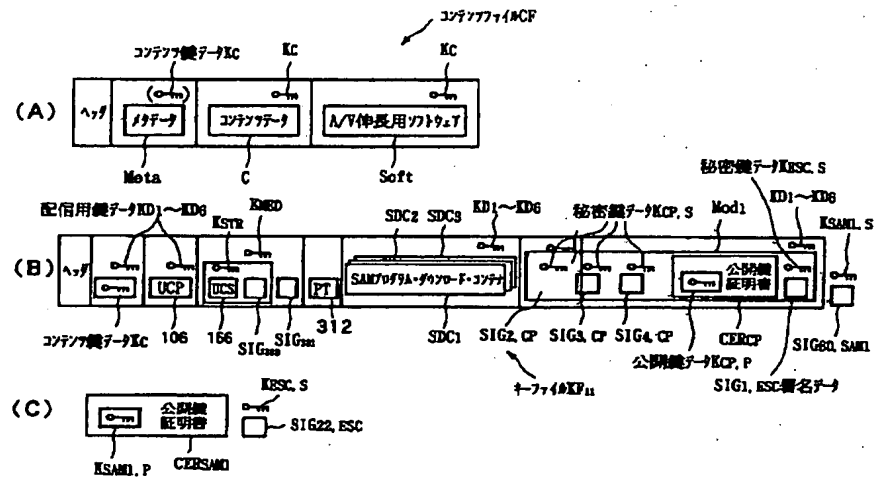


【図 4 4】

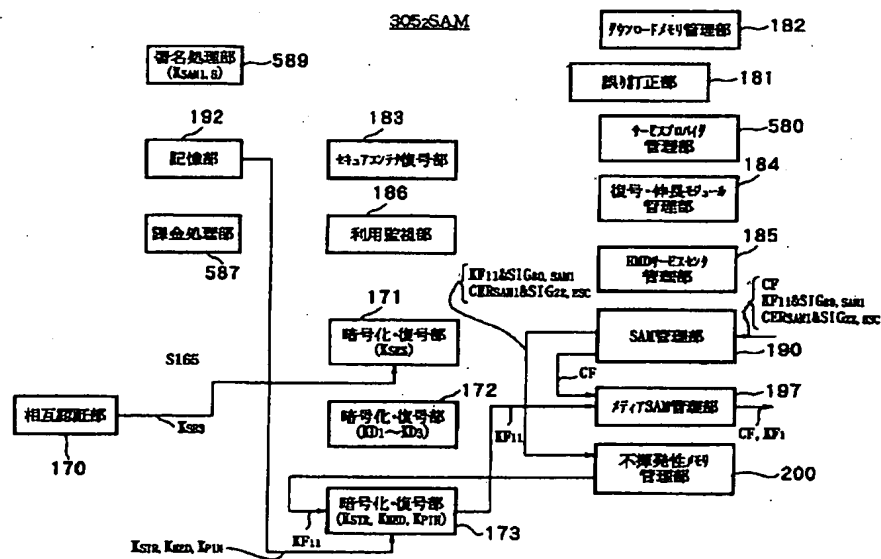


[illegible][illegible]

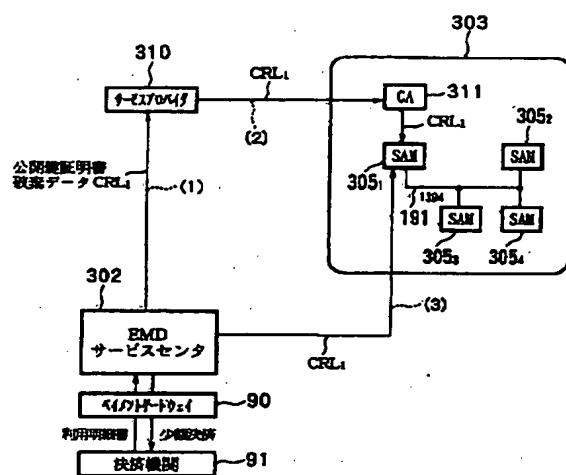
【図50】



【図51】

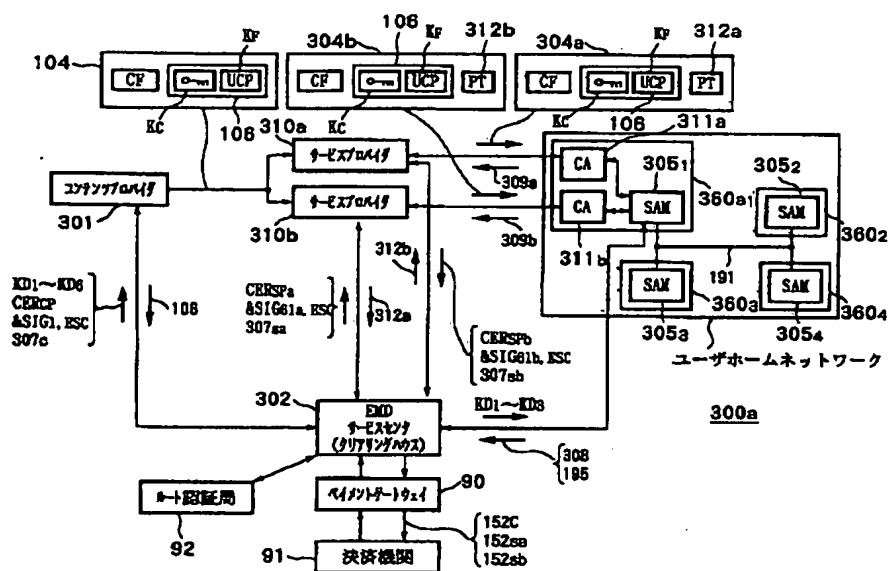


【图 5 9】

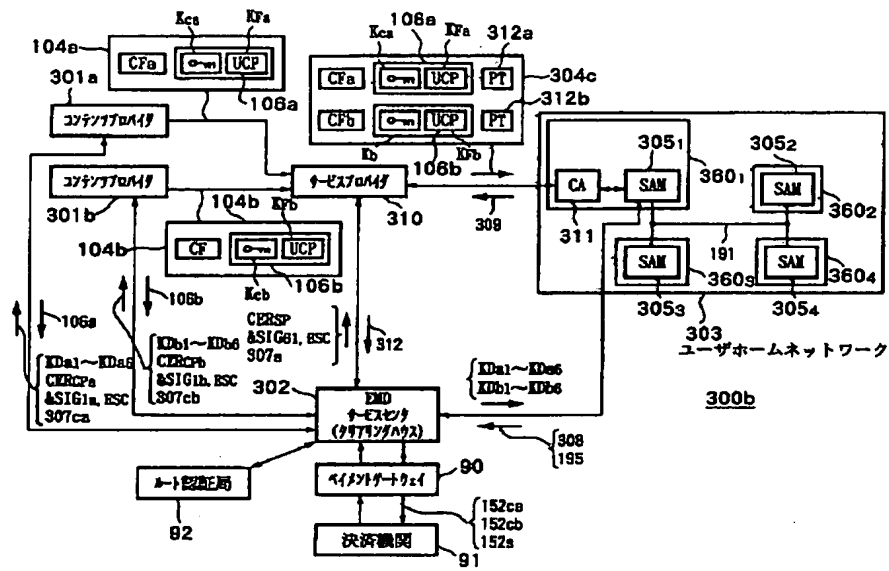


CEROPを無効にする場合

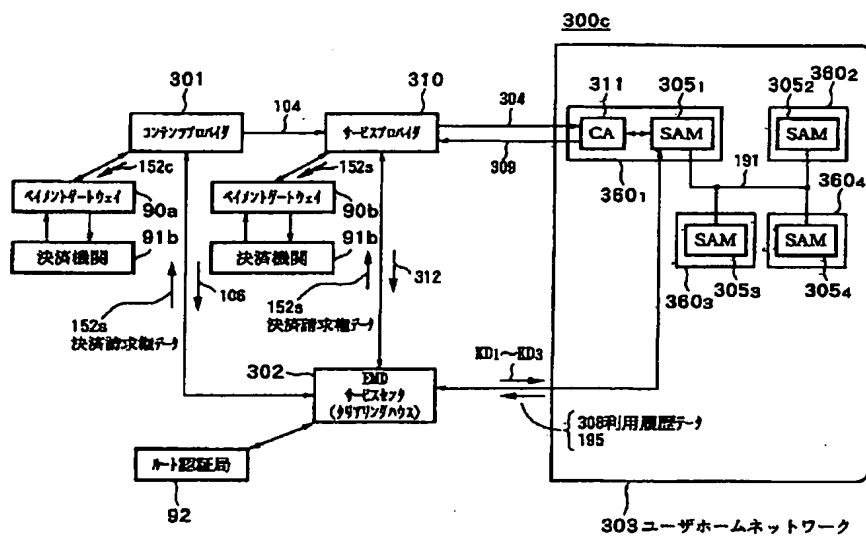
【图 5 4】



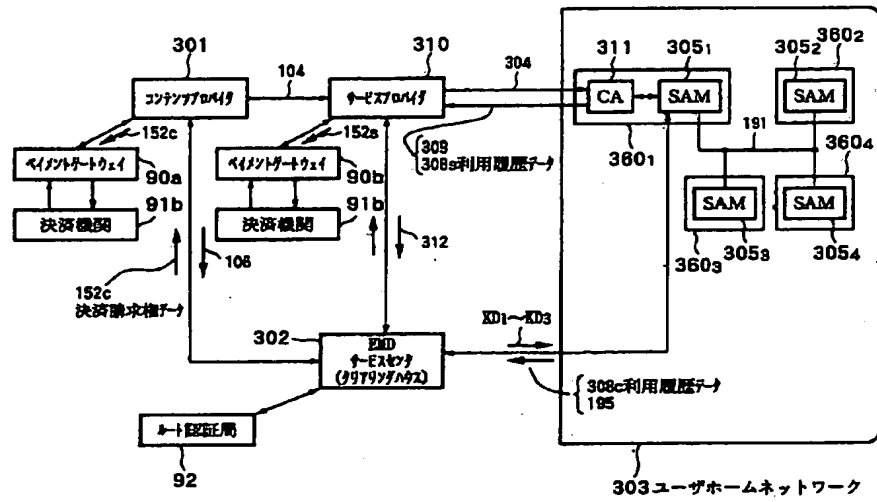
【図55】



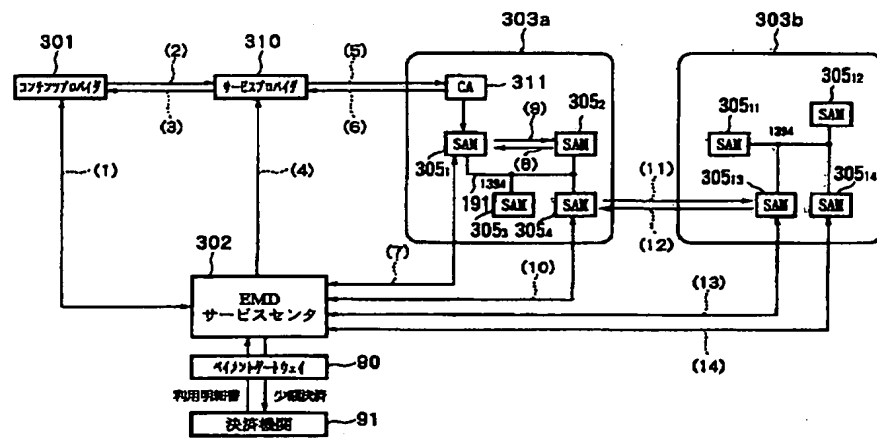
【図56】



【図57】

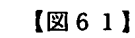


【図58】

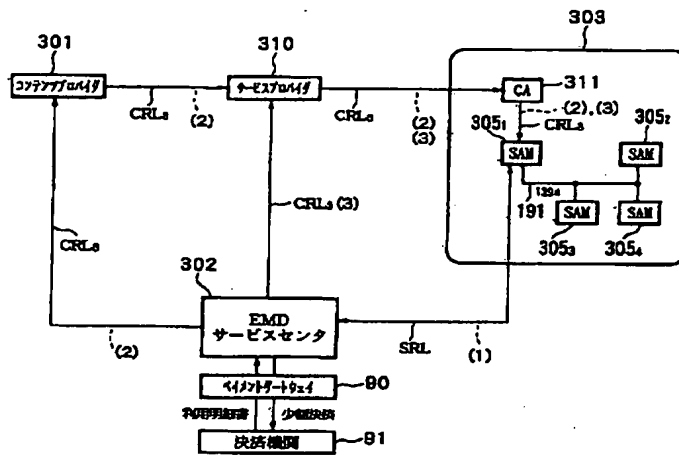


公開鍵証明書の入手ルート

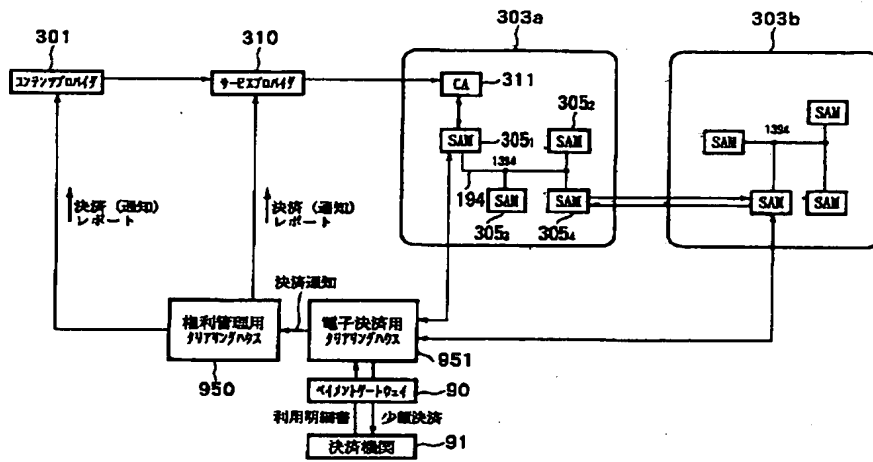
CERspを無効にする場合



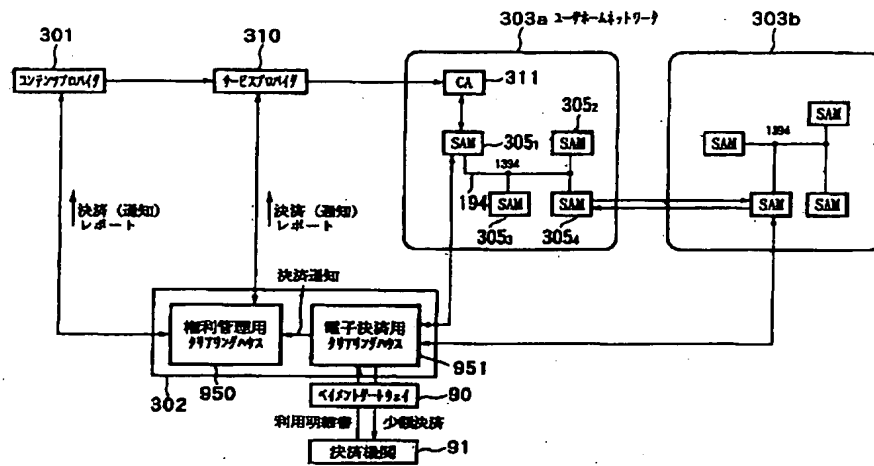
【图 6 2】



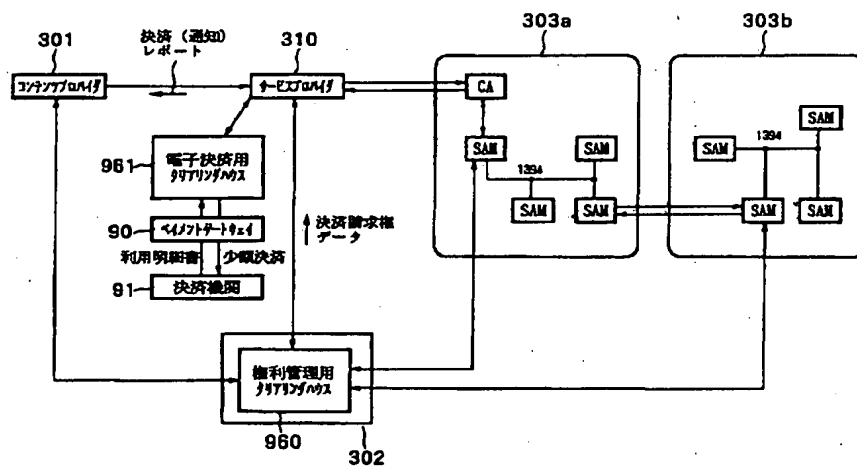
【図 6 3】



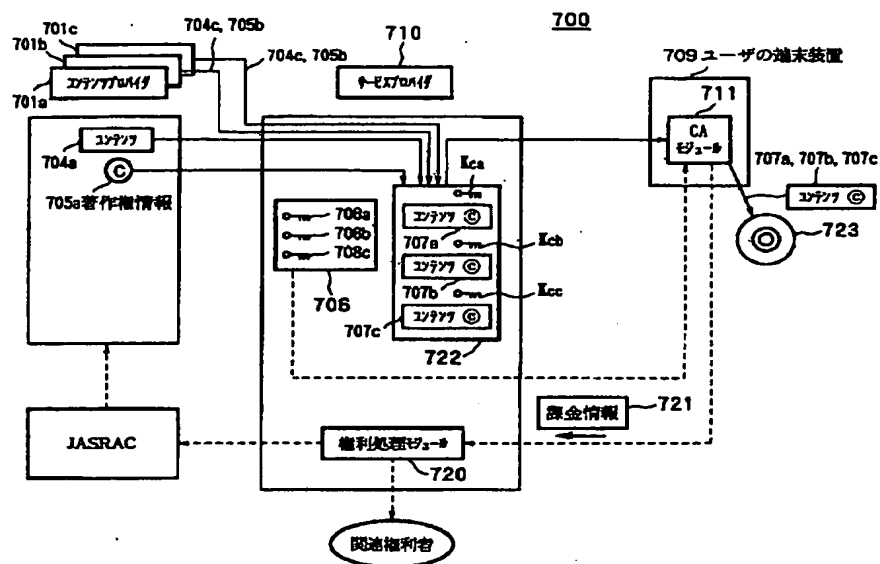
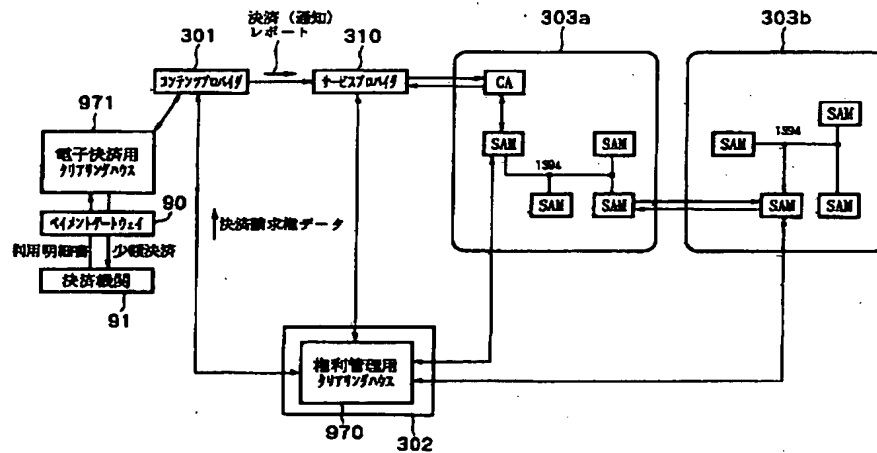
【図64】



【図65】



【圖 6 7】



テーマコード*(参考)

				Z
6	0	1	B	
6	7	5	B	
6	7	5	D	

F ターム(参考) 5B049 AA05 BB11 BB46 CC05 CC36
DD05 EE03 EE05 EE59 FF09
GG04 GG07 GG10
5B089 GA11 GA21 GB04 HA10 JB22
KA15 KA17 KB13 KC58
5D044 AB05 DE48 GK12 GK17 HL11
5J104 AA07 AA09 AA14 KA01 LA03
LA06 MA02 PA07
9A001 CC02 EE03 EE04 HH15 KK43
LL03